(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年6 月14 日 (14.06.2001)

PCT

(10) 国際公開番号
WO 01/43342 A1

(51) 国際特許分類[7]: H04L 9/32, G06F 12/14, G10K 15/02, G06F 13/00

(21) 国際出願番号: PCT/JP00/08593

(22) 国際出願日: 2000 年12 月5 日 (05.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/346861 1999 年12 月6 日 (06.12.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気ヌ98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 吉岡 誠 (YOSHIOKA, Makoto) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (P).

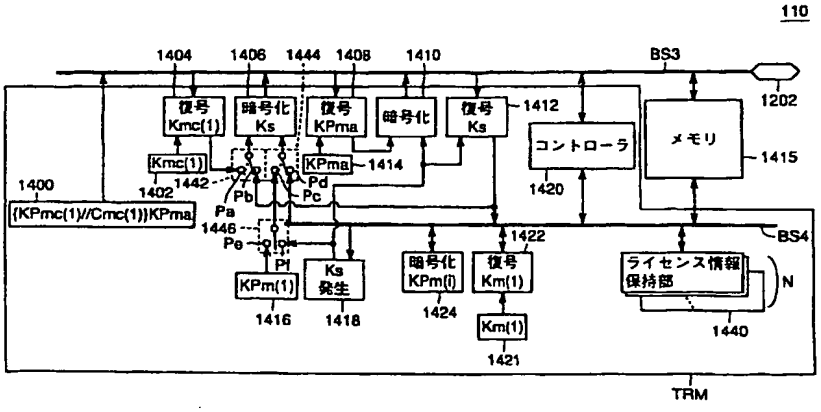
(74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.) ; 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN

(54) 発明の名称: データ配信システムおよびそれに使用される記録装置




1404...DECRYPTION Kmc(1)
1406...ENCRYPTION Ks
1408...DECRYPTION KPma
1410...ENCRYPTION
1412...DECRYPTION Ks
1420...CONTROLLER
1415...MEMORY
1418...Ks GENERATION
1424...ENCRYPTION KPm(i)
1422...DECRYPTION Km(1)
1440...LICENSE INFORMATION HOLDING

(57) Abstract: A memory card (110) stores access limit information (AC1) in a license information holding section (1440) in a TRM area. The access limit information (AC1) includes information concerning the number of possible reproductions and the number of possessed licenses. A controller (1420) confirms the access limit information (AC1), reproduces and transfers a content, updates it as necessary, and stores the updated access limit information (AC1) in the license information holding section (1440).

[続葉有]

WO 01/43342 A1

(19)日本国特許庁（ＪＰ）　**再公表特許（Ａ１）**　(11)国際公開番号

**ＷＯ０１／０４３３４２**

発行日　平成15年６月17日(2003.6.17)　(43)国際公開日　平成13年６月14日(2001.6.14)

| (51)Int.Cl.[7] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | Ｇ０６Ｆ | 15/00 | ３３０Ｚ |
| | 12/14 | ３２０ | | 12/14 | ３２０Ｆ |
| | 17/60 | １４２ | | 17/60 | １４２ |
| | | ３０２ | | | ３０２Ｅ |
| | | ５１２ | | | ５１２ |

審査請求　有　予備審査請求　有　（全104頁）　最終頁に続く

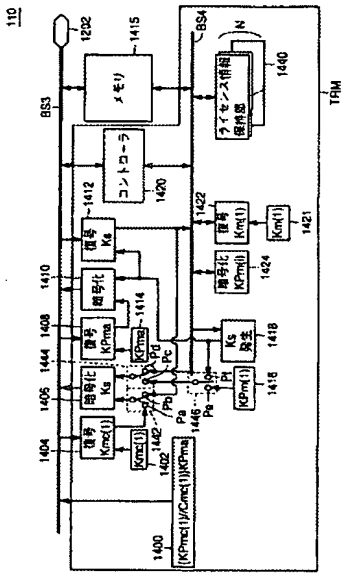
出願番号　特願2001－542929(P2001－542929)
(21)国際出願番号　ＰＣＴ／ＪＰ００／０８５９３
(22)国際出願日　平成12年12月５日(2000.12.5)
(31)優先権主張番号　特願平11－346861
(32)優先日　平成11年12月６日(1999.12.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(71)出願人　株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２
(71)出願人　富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(74)代理人　弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ配信システムおよびそれに使用される記録装置

(57)【要約】
メモリカード（１１０）は、ＴＲＭ領域内のライセンス情報保持部（１４４０）にアクセス制限情報（ＡＣ１）を格納する。アクセス制限情報（ＡＣ１）は、再生可能回数および所有ライセンス数等の情報を有する。コントローラ（１４２０）は、コンテンツの再生および移動動作時においては、アクセス制限情報（ＡＣ１）を確認した上で、再生および移動を実行し、実行後は必要に応じて、アクセス制限情報（ＡＣ１）を更新してライセンス情報保持部（１４４０）に格納する。



【特許請求の範囲】

【請求項１】　データ配信システムであって、

暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）と、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Ｄａｔａ）を得るための復号鍵であるライセンスキー（Ｋｃ）を配信するためのコンテンツ供給装置（１０，１１）と、

前記コンテンツ供給装置からの前記配信を受ける複数の端末（１００，１０１）とを備え、

前記コンテンツ供給装置は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

前記配信が要求された場合において、アクセス制限情報（ＡＣ１）を生成して、少なくとも前記ライセンスキーを含む再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）と前記アクセス制限情報とを前記第１のインタフェース部を介して出力するための配信制御部（３１５）とを含み、

各前記端末は、

外部との間でデータを授受するための第２のインタフェース部（１１０２）と、

前記第２のインタフェース部を介して、前記暗号化コンテンツデータと前記再生情報と前記アクセス制限情報とを受けて記録する配信データ解読部（１１０，２１０）とを含み、

前記配信データ解読部は、

前記暗号化コンテンツデータ、前記再生情報および前記アクセス制限情報を記録するための記憶部（１４１５，１４３０，１４４０）と、

外部から前記再生情報の出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記出力の可否を判断する制御部（１４２０）とを有する、データ配信システム。

【請求項２】　各前記端末（１００，１０１）は、コンテンツ再生部をさらに含み、

前記コンテンツ再生部は、

外部からコンテンツデータの再生動作が指示された場合において、前記配信デ

ータ解読部（１１０，２１０）から前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）を受けて、前記ライセンスキー（Ｋｃ）によって前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部（１５１６，１５１８）を有し、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読部から前記コンテンツ再生部への、前記再生情報の出力回数を制限する再生制御情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記制御部（１４２０）は、前記再生動作が指示された場合において、前記記憶部に記録された前記再生制御情報に基づいて、前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新できる、請求の範囲第１項に記載のデータ配信システム。

【請求項３】　前記アクセス制限情報（ＡＣ１）は、前記配信データ解読部（１１０，２１０）から他の配信データ解読部（１１２）に対しての、前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の複製可能回数を制限する複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記制御部（１４２０）は、他の配信データ解読部に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記記憶部に記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新できる、請求の範囲第１項に記載のデータ配信システム。

【請求項４】　前記コンテンツ供給装置（１０，１１）は、

認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記配信データ解読部（１１０，２１０）に対応して予め定められる第１の公開暗号鍵（ＫＰｍｃ（ｍ））を、前記第１のインタフェース部（３５０）を介して受けて復号処理するための第１の復号処理部（３１２）と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される第１の共通鍵（Ｋｓ１）を生成する第１のセッションキー生成部（３１６）と、

前記第１の共通鍵によって暗号化されて、前記第１のインタフェース部を介し

て返信される第２の公開暗号鍵（ＫＰｍ（ｉ））および第２の共通鍵（Ｋｓ２）を復号抽出するためのセッションキー復号部（３２０）と、

前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記アクセス制限情報（ＡＣ１）を、前記セッションキー復号部により復号された前記第２の公開暗号鍵によって暗号化する第１のライセンスデータ暗号化処理部（３２６）と、

前記第１のライセンスデータ暗号化処理部の出力を、前記セッションキー復号部により復号された前記第２の共通鍵によってさらに暗号化して前記第１のインタフェース部に与え配信するための第２のライセンスデータ暗号化処理部（３２８）とをさらに含み、

前記配信データ解読部（１１０，２１０）は、

前記認証鍵によって復号可能な状態に暗号化された、前記配信データ解読部に対応して定められる前記第１の公開暗号鍵を保持し、少なくとも前記ライセンスキーを受信する場合に出力する第１の認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号するための第１の秘密復号鍵（Ｋｍｃ（ｍ））を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号鍵によって暗号化された前記第１の共通鍵を受けて、前記第１の秘密復号鍵によって復号処理するための第１の復号処理部（１４０４）と、

前記第２の公開暗号鍵を保持する第２の鍵保持部（１４１６）と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される前記第２の共通鍵（Ｋｓ２）を生成する第２のセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記第２のインタフェース部（１２０２）に出力するための第１の暗号化処理部（１４０６）と、

前記コンテンツ供給装置から配信される、前記第２の共通鍵および前記第２の公開暗号鍵によって暗号化された、前記再生情報および前記アクセス制限情報を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２

）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Ｋｍ（ｉ））を保持する第３の鍵保持部（１４２１）と、

暗号化された、前記再生情報および前記アクセス制限情報を、第２の秘密復号鍵によって復号するための第３の復号処理部（１４２２）とをさらに有し、

前記記憶部（１４１５，１４３０，１４４０）は、前記再生情報を、前記第２の公開暗号鍵によって暗号化された状態および前記第３の復号処理部によって復号された状態のいずれか一方の状態で記録するための第１の記憶ブロック（１４１５，１４３０）と、

前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを有する、請求の範囲第１項に記載のデータ配信システム。

【請求項５】　前記第２のセッションキー発生部（１４１８）は、外部から指示されるコンテンツデータの再生動作に応じて、第３の共通鍵（Ｋｓ３）を生成し、

前記記憶部（１４１５，１４３０，１４４０）は、前記制御部（１４２０）に制御されて、前記再生動作が指示されるのに応じて、前記暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）および前記再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記再生動作において、前記第１の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を抽出し、

前記第２の復号処理部（１４１２）は、前記再生動作において、前記第３の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記再生情報の通信ごとに更新される第４の共通鍵（Ｋｓ４）を抽出し、

前記第１の暗号化処理部（１４０６）は、前記再生動作において、前記第３の復号処理部および前記第１の記憶ブロックのいずれか一方から前記再生情報を受けて、前記第２の復号処理部（１４１２）で抽出された前記第４の共通鍵によって暗号化し、

各前記端末（１００，１０１）は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

前記認証鍵によって復号可能な状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第３の公開暗号鍵（ＫＰｐ（ｉ））を保持し、前記再生動作に応じて前記配信データ解読部に対して出力する第２の認証データ保持部（１５００）と、

前記第４の共通鍵を生成する第３のセッションキー発生部（１５０８）と、

前記配信データ解読部から送信される、前記第４の共通鍵によって暗号化された前記再生情報から前記再生情報を復号抽出するための第４の復号処理部（１５１０）と、

前記再生動作が指示された場合において、前記配信データ解読部（１１０，２１０）からの前記暗号化コンテンツデータを受けて、前記再生情報に含まれる前記ライセンスキー（Ｋｃ）により前記暗号化コンテンツデータを復号して再生するためのコンテンツデータ再生部（１５１６，１５１８）と、

前記第３の公開暗号鍵によって暗号化されたデータを復号化するための第３の秘密復号鍵（Ｋｐ（ｉ））を保持する第４の鍵保持部（１５０２）と、

前記第３の公開暗号鍵によって暗号化されて前記配信データ解読部から返信されるデータを復号して前記第３の共通鍵を得るための第５の復号処理部（１５０４）と、

前記第５の復号処理部から受ける前記第３の共通鍵によって、前記第４の共通鍵を暗号化して前記配信データ解読部に対して出力する第２の暗号化処理部（１５０６）とを有し、

前記配信データ解読部は、

暗号化された前記第３の公開暗号鍵を前記コンテンツ再生部から受けて、前記認証鍵によって復号処理するための認証処理部（１４０８）と、

前記制御部に制御されて、前記認証処理部から受ける前記第３の公開暗号鍵によって前記第３の共通鍵を暗号化して、対応する前記コンテンツ再生部に対して出力する第３の暗号化処理部（１４１０）とをさらに有し、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読部から前記コンテンツデータ再生部への、前記再生情報の出力回数を制限する再生制御情報（Ｓｕｂ

＿Ｍｏｖｅ）を含み、

前記制御部（１４２０）は、前記再生動作が指示された場合において前記配信データ解読部の各部の動作を制御し、前記第２の記憶ブロックに記録された前記再生制御情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新可能である、請求の範囲第４項に記載のデータ配信システム。

【請求項６】　前記認証処理部（１４０８）は、他の配信データ解読部（１０２）に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記他の配信データ解読部に対応する前記第１の公開暗号鍵（ＫＰｍｃ（ｍ））を復号処理によって取得し、

前記配信データ解読部および前記他の配信データ解読部にそれぞれ対応する複数の前記第２のセッションキー発生部は、外部から指示される前記複製動作に応じて、前記第３および第２の共通鍵（Ｋｓ３，Ｋｓ２）をそれぞれ生成し、

前記第３の暗号化処理部（１４１０）は、前記複製動作において、前記他の配信データ解読部に対応する前記第１の公開暗号鍵によって、前記配信データ解読部に対応する前記第３の共通鍵を暗号化して前記他の配信データ解読部に対して出力し、

前記第２の復号処理部（１４１２）は、前記複製動作において、前記配信データ解読部に対応する前記第３の共通鍵で暗号化されて前記他の配信データ解読部から返信されるデータを復号して、前記他の配信データ解読部で生成された前記第２の共通鍵および前記他の配信データ解読部に対応する前記第２の公開暗号鍵（ＫＰｍ（ｉ））を取得し、

前記第１の記憶ブロック（１４１５，１４３０）は、前記制御部（１４２０）に制御されて、前記複製動作が指示されるのに応じて、前記再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記複製動作において、前記第１の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を抽出し、

前記配信データ解読部（１１０，２１０）は、

前記複製動作が外部から指示された場合において、前記第３の復号処理部およ

び前記第１の記憶ブロックのいずれか一方から受けた前記再生情報を、前記他の配信データ解読部に対応する前記第２の公開暗号鍵によって暗号化するための第４の暗号化処理部（１４２４）をさらに有し、

前記第１の暗号化処理部（１４０６）は、前記複製動作において、前記第２の復号処理部（１４１２）によって取得された前記第２の共通鍵と、前記第４の暗号化処理部の出力とを受けて、前記第４の暗号化処理部の出力を前記第２の共通鍵によってさらに暗号化して前記他の配信データ解読部に出力し、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読部から他の配信データ解読部に対しての、前記再生情報の複製可能回数を制限する複製制限情報（Ｓｕｂ＿ｍｏｖｅ）を含み、

前記制御部（１４２０）は、前記複製動作時において前記配信データ解読部の各部の動作を制御し、前記第２の記憶ブロックに記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新する、請求の範囲第５項に記載のデータ配信システム。

【請求項７】　前記コンテンツ供給装置（１０）は、

前記コンテンツ再生部にて再生可能な共通秘密鍵（Ｋｃｏｍ）を保持する第５の鍵保持部（３２２）と、

前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を前記共通秘密鍵によって暗号化し、前記第１のライセンスデータ暗号化処理部（３２６）に対して出力する第３のライセンスデータ暗号化部（３２４）とをさらに含み、

前記コンテンツ再生部は、

前記共通秘密鍵を保持する第６の鍵保持部（１５１２）と、

前記第４の復号処理部（１５１０）の出力を受けて、前記第６の鍵保持部に保持された前記共通秘密鍵によって前記再生情報を復号し、前記ライセンスキー（Ｋｃ）を抽出して前記コンテンツデータ再生部（１５１６，１５１８）に対して出力するための第６の復号処理部（１５１４）をさらに有する、請求の範囲第５項に記載のデータ配信システム。

【請求項８】　前記コンテンツ供給装置（１０）は、

前記コンテンツデータ再生部にて再生可能な第４の公開暗号鍵を保持する第５の鍵保持部と、

前記再生情報を前記第４の公開暗号鍵にて暗号化し、前記第１のライセンスデータ暗号化処理部に対して出力する第３のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第４の公開暗号鍵によって暗号化された前記再生情報を復号できる第４の秘密復号鍵を保持する第６の鍵保持部と、

前記第４の復号処理部の出力を受けて、前記第６の鍵保持部に保持された前記第４の秘密復号鍵によって前記再生情報（ＡＣ／／Ｋｃ２）を復号し、前記ライセンスキー（Ｋｃ）を抽出して前記コンテンツデータ再生部（１５１６，１５１８）に対して出力するための第６の復号処理部をさらに含む、請求の範囲第５項に記載のデータ配信システム。

【請求項９】　前記配信データ解読部（１１０，２１０）は、前記端末（１００，１０１）に着脱可能な記録装置である、請求の範囲第１項に記載のデータ配信システム。

【請求項１０】　前記記録装置は、メモリカードである、請求の範囲第９項に記載のデータ配信システム。

【請求項１１】　前記第１のインタフェース部（３５０）と前記第２のインタフェース部（１２０２）とは、携帯電話網によって接続される、請求の範囲第１項に記載のデータ配信システム。

【請求項１２】　前記記憶部（１４１５，１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１３】　前記記憶部（１４１５，１４３０，１４４０）は、

前記暗号化コンテンツデータを記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを含み、

前記第１の記憶ブロックは、前記再生情報を暗号化された状態でさらに記録し、

前記第２の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１４】　前記記憶部（１４１５，１４３０，１４４０）は、

前記暗号化コンテンツデータを記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報および前記再生情報を記録するための第２の記憶ブロック（１４３０，１４４０）とを含み、

前記第２の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１５】　前記配信制御部（３１５）は、配信先の前記配信データ解読部（１１０，１２０）を認証した後に、前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）と前記アクセス制限情報（ＡＣ１）とを前記第１のインタフェース部（３５０）を介して出力する、請求の範囲第１項に記載のデータ配信システム。

【請求項１６】　前記配信データ解読部（１１０，１２０）は、外部から前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力が指示された場合に、出力先を認証した後に、前記再生情報を前記第２のインタフェース部（１１０２）を介して出力する、請求の範囲第１項に記載のデータ配信システム。

【請求項１７】　前記制御部（１４２０）は、前記複製動作において、他の配信データ解読部（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の配信データ解読部に対して出力する、請求の範囲第３項に記載のデータ配信システム。

【請求項１８】　前記制御部（１４２０）は、前記複製動作において、他の配信

データ解読部（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第４の暗号化処理部は、変更した前記アクセス制限情報を暗号化して、前記再生情報とともに前記第１の暗号化処理部へ与える、請求の範囲第６項に記載のデータ配信システム。

【請求項１９】　記録装置であって、

外部との間でデータを授受するためのインタフェース部（１２０２）と、

前記インタフェース部を介して入力される、格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記格納データの前記記録装置からの出力を制御するためのアクセス制限情報（ＡＣ１）を記録するための記憶部（１４１５，１４３０，１４４０）と、

外部から前記格納データの出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記出力の可否を判断する制御部（１４２０）とを備える、記録装置。

【請求項２０】　前記アクセス制限情報（ＡＣ１）は、前記記録装置から他の機器（１００，１０１）への前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力回数を制限する出力回数制御情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記制御部（１４２０）は、前記他の機器に対する前記格納データの出力が指示された場合において、前記出力回数制御情報に基づいて前記出力の可否を判断するとともに、前記出力後、必要に応じて前記出力回数制御情報を更新可能である、請求の範囲第１９項に記載の記録装置。

【請求項２１】　前記アクセス制限情報（ＡＣ１）は、他の前記記録装置（１１２）に対する前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の複製可能回数を制限する複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記制御部（１４２０）は、前記他の記録装置に対する前記格納データの複製指示が外部から指示された場合において、前記複製制限情報に基づいて前記格納データの出力の可否を判断するとともに、前記出力後、必要に応じて前記複製制限情報を更新可能である、請求の範囲第１９項に記載の記録装置。

【請求項２２】　前記記憶部は、前記アクセス制限情報（ＡＣ１）を記録するための記憶ブロック（１４４０）を有し、

前記記録装置は、

前記記録装置に対応して予め定められる公開暗号鍵（ＫＰｍ（ｉ））によって暗号化されたデータを復号するための秘密復号鍵（Ｋｍ（ｉ））を保持する秘密鍵保持部（１４２１）と、

前記インタフェース部（１２０２）を介して入力される、前記公開暗号鍵によって暗号化された前記アクセス制限情報（ＡＣ１）を復号して、前記記憶ブロックに与えるアクセス制限情報復号部（１４２２）とをさらに備える、請求の範囲第１９項に記載の記録装置。

【請求項２３】　前記記憶ブロック（１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第２２項に記載の記録装置。

【請求項２４】　認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記記録装置に対応して定められる第１の公開暗号鍵（ＫＰｍｃ（ｍ））を保持し、前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記アクセス制限情報（ＡＣ１）を受信する場合において前記インタフェース部（１２０２）を介して外部に出力する認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵（Ｋｍｃ（ｍ））を保持する第１の鍵保持部（１４４２）と、

前記第１の公開暗号鍵によって暗号化された第１の共通鍵（Ｋｓ１）を前記インタフェース部を介して外部から受けて、復号処理するための第１の復号処理（１４０４）と、

前記記録装置ごとに異なる第２の公開暗号鍵（ＫＰｍ（ｉ））を保持する第２の鍵保持部（１４１６）と、

前記格納データの通信ごとに更新される第２の共通鍵（Ｋｓ２）を生成するセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記インタフェース部を介して外部に出力するための第１の暗号化処理部（１４０６）と、

前記インタフェース部を介して、前記第２の共通鍵および前記第２の公開暗号鍵によって暗号化されて入力される前記格納データおよび前記アクセス制限情報を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Ｋｍ（ｉ））を保持する第３の鍵保持部（１４２１）と、

暗合化された、前記格納データおよび前記アクセス制限情報を、前記第２の秘密復号鍵によって復号するための第３の復号処理部（１４２２）とをさらに備え、

前記記憶部（１４１５，１４３０，１４４０）は、前記格納データを、前記第２の公開暗号鍵によって暗号化された状態および、前記第３の復号処理部によって復号された状態のいずれか一方の状態で記録する、請求の範囲第１９項に記載の記録装置。

【請求項２５】　前記セッションキー発生部（１４１８）は、外部から指示される、他の機器（１００，１０１）への前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力指示である第１の出力指示に応じて、第３の共通鍵（Ｋｓ３）を生成し、

前記記録装置は、

前記認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記他の機器に対応して予め定められる第３の公開暗号鍵（ＫＰｐ（ｎ））を前記インタフェース部（１２０２）を介して受けて、前記認証鍵によって復号処理するための認証処理部（１４０８）と、

前記第１の出力指示に応じて、前記認証処理部から受ける前記第３の公開暗号鍵によって前記第３の共通鍵を暗号化して、前記他の機器に対して出力する第２

の暗号化処理部（１４１０）とをさらに備え、

前記インタフェース部は、前記第１の出力指示に応じて、前記第３の共通鍵によって暗号化されて返信される、前記他の機器において生成された第４の共通鍵（Ｋｓ４）を受けて前記第２の復号処理部（１４１２）に伝達し、

前記第２の復号処理部は、前記第１の出力指示に応じて、前記セッションキー発生部から受けた前記第３の共通鍵によって、前記第３の共通鍵によって暗号化された前記第４の共通鍵を抽出し、

前記記憶部は、前記制御部（１４２０）に制御されて、前記第１の出力指示に応じて、前記格納データを出力し、

前記第３の復号処理部（１４２２）は、前記第１の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって前記格納データを抽出し、

前記第２の復号処理部（１４１２）は、前記第１の出力指示に応じて、前記第３の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記格納データの通信ごとに更新される第４の共通鍵（Ｋｓ４）を抽出し、

前記第１の暗号化処理部（１４０６）は、前記第１の出力指示に応じて、前記第３の復号処理部および前記記憶部のいずれか一方から前記格納データを受けて、前記第２の復号処理部（１４１２）で抽出された前記第４の共通鍵によって暗号化して、前記インタフェース部を介して前記他の機器に出力し、

前記アクセス制限情報（ＡＣ１）は、前記記録装置から他の機器への前記格納データの出力回数を制限する出力回数制御情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記制御部（１４２０）は、前記第１の出力指示に応じて前記記録装置内の各部の動作を制御し、前記出力回数制御情報に基づいて前記格納データの出力の可否を判断し、前記格納データの出力後、必要に応じて前記出力回数制御情報を更新する、請求の範囲第２４項に記載の記録装置。

【請求項２６】　前記セッションキー発生部（１４１８）は、外部から指示される、前記記録装置から他の記録装置（１１２）への前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力指示である第２の出力指示に応じて

、前記第３の共通鍵（Ｋｓ３）を生成し、

前記認証処理部（１４０８）は、前記第２の出力指示に応じて、前記他の記録装置に対応する前記第１の公開暗号鍵（ＫＰｍｃ（ｍ））を復号処理によって取得し、

前記第２の暗号化処理部（１４１０）は、前記第２の出力指示に応じて、前記他の記録装置に対応する前記第１の公開暗号鍵によって、前記記録装置に対応する前記第３の共通鍵を暗号化して前記他の記録装置に対して出力し、

前記第２の復号処理部（１４１２）は、前記第２の出力指示に応じて、前記記録装置に対応する前記第３の共通鍵で暗号化されて前記他の記録装置から返信されるデータを復号して、前記他の記録装置で生成された前記第２の共通鍵（Ｋｓ２）および前記他の記録装置に対応する前記第２の公開暗号鍵（ＫＰｍ（ｉ））を取得し、

前記記憶部は、前記制御部（１４２０）に制御されて、前記第２の出力指示に応じて、前記格納データを出力し、

前記第３の復号処理部（１４２２）は、前記第２の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって前記格納データを抽出し、

前記記録装置は、

前記第２の出力指示がなされた場合において、前記第３の復号処理部および前記記憶部のいずれか一方から受けた前記格納データを、前記他の記録装置に対応する前記第２の公開暗号鍵によって暗号化するための第３の暗号化処理部（１４２４）をさらに有し、

前記第１の暗号化処理部（１４０６）は、前記第２の出力指示に応じて、前記第３の暗号化処理部の出力を、前記他の記録装置で生成された前記第２の共通鍵によってさらに暗号化して、前記インタフェース部を介して前記他の記録装置に出力し、

前記アクセス制限情報（ＡＣ１）は、前記他の記録装置に対する前記格納データの出力可能回数を制限する複製制限情報を含み、

前記制御部（１４２０）は、前記第２の出力指示に応じて前記記録装置内の各

部の動作を制御し、前記複製制限情報に基づいて前記第２の出力指示の実行の可否を判断し、前記第２の出力指示の実行後において、必要に応じて前記複製制限情報を更新する、請求の範囲第２５項に記載の記録装置。

【請求項２７】　前記記憶部（１４１５，１４３０，１４４０）は、前記インタフェース部（１２０２）を介して外部から入力される暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）をさらに記録し、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）は、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Ｄａｔａ）を得るための復号鍵であるライセンスキー（Ｋｃ）を含む、請求の範囲第１９項に記載の記録装置。

【請求項２８】　前記記録装置は、メモリカードである、請求の範囲第１９項に記載の記録装置。

【請求項２９】　前記記憶部（１４１５，１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１９に記載の記録装置。

【請求項３０】　記憶部（１４１５，１４３０，１４４０）は、

外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される第１の記憶ブロック（１４３０，１４４０）と、

外部から直接アクセス可能な第２の記憶ブロック（１４１５）とを含み、

前記アクセス制限情報（ＡＣ１）は、前記第１の記憶ブロックに記録され、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）は、暗号化されて前記第２の記憶ブロックに記録される、請求の範囲第１９項に記載の記録装置。

【請求項３１】　記憶部（１４１５，１４３０，１４４０）は、

外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される第１の記憶ブロック（１４３０，１４４０）と、

外部から直接アクセス可能な第２の記憶ブロック（１４１５）とを含み、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）およびアクセス制限情報（ＡＣ１）は、前記第１の記憶ブロックに記録される、請求の範囲

第１９項に記載の記録装置。

【請求項３２】　前記制御部（１４２０）は、前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力を指示された場合に、出力先を認証した後に、前記格納データを出力する、請求の範囲第１９項に記載の記録装置。

【請求項３３】　前記制御部（１４２０）は、他の記録装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の記録装置に対して出力する、請求の範囲第２１項に記載の記録装置。

【請求項３４】　前記制御部（１４２０）は、前記第２の出力指示において、他の記録装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第３の暗号化処理部は、前記格納データとともに、変更した前記アクセス制限情報を暗号化し、前記第１の暗号化処理部へ与える、請求の範囲第２６項に記載の記録装置。

【発明の詳細な説明】

技術分野

本発明は、携帯電話機等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムおよび当該システムで使用されるメモリカードに関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額

を間接的に著作権者に対して保証金として支払うことになっている。

しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化のほとんどないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽データをコピーすることは、著作権保護のために機器の構成上できないようになっている。

このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信されるコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

発明の開示

この発明の目的は、情報通信網、たとえば携帯電話機等の情報通信網を介してコンテンツデータを配信することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明の他の目的は、配信されたコンテンツデータが、著作権者の許可なく複製されることを防止することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

この発明に従うデータ配信システムは、複数の端末と、コンテンツ供給装置とを備える。コンテンツ供給装置は、外部との間でデータを授受するための第１のインタフェース部と、配信が要求された場合において、アクセス制限情報を生成して、少なくともライセンスキーを含む再生情報とアクセス制限情報とを第１のインタフェース部を介して出力するための配信制御部とを含む。各端末は、外部との間でデータを授受するための第２のインタフェース部と、第２のインタフェース部を介して、暗号化コンテンツデータと再生情報とアクセス制限情報とを受けて記録する配信データ解読部とを含む。配信データ解読部は、暗号化コンテンツデータ、再生情報およびアクセス制限情報を記録するための記憶部と、外部か

ら再生情報の出力が指示された場合に、記憶部に記録されたアクセス制限情報に基づいて出力の可否を判断する制御部とを有する。

好ましくは、各端末は、コンテンツ再生部をさらに含み、コンテンツ再生部は、外部からコンテンツデータの再生動作が指示された場合において、配信データ解読部から再生情報および暗号化コンテンツデータを受けて、ライセンスキーによって暗号化コンテンツデータを復号して再生するコンテンツデータ再生部を有する。アクセス制限情報は、配信データ解読部からコンテンツ再生部への、再生情報の出力回数を制限する再生制御情報を含む。制御部は、再生動作が指示された場合において、再生制御情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後に必要に応じて再生制御情報を更新する。

好ましくは、アクセス制限情報は、配信データ解読部から他の配信データ解読部に対しての、再生情報の複製可能回数を制限する複製制限情報を含む。制御部は、他の配信データ解読部に対して再生情報を複製する複製動作が外部から指示された場合において、複製制限情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後において、必要に応じて所有ライセンス数情報を更新可能である。

このようなデータ配信システムにおいては、再生可能回数や所有ライセンス数に関するアクセス制限情報を、配信サーバを介さずに、配信データ解読部、より詳しくはメモリカードの内部において、保持および更新できる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができる。この結果、再生情報として再生回路の制限付き再生権の発行が可能となり、試聴用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティー強度を確保できるため、著作権者の権利をも守ることができるようになる。

この発明の別の局面に従うと、記録装置は、インタフェース部と、記憶部と、制御部とを備える。インタフェース部は、外部との間でデータを授受する。記憶

部は、インタフェース部を介して入力される、格納データおよび格納データの記録装置からの出力を制御するためのアクセス制限情報（ＡＣ１）を記録する。制御部は、外部から格納データの出力が指示された場合に、アクセス制限情報に基づいて出力の可否を判断する。

好ましくは、アクセス制限情報は、記録装置から他の機器への格納データの出力回数を制限する出力回数制御情報を含み、制御部は、他の機器に対する格納データの出力が指示された場合において、出力回数制御情報に基づいて出力の可否を判断するとともに、出力後に必要に応じて出力回数制御情報を更新可能である。

好ましくは、アクセス制限情報は、他の記録装置に対する格納データの複製可能回数を制限する複製制限情報を含み、制御部は、他の記録装置に対する格納データの複製指示が外部から指示された場合において、所有ライセンス数情報に基づいて格納データの出力の可否を判断し、出力後において、必要に応じて複製制限情報を更新可能である。

このような記録装置においては、複製制限情報および出力回数制御情報といったアクセス制限情報を、配信サーバを介さずに記憶領域内部で保持および更新することができる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができる。この結果、再生回路の制限付き再生権の発行が可能となり、試聴用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティー強度を確保できるため、著作権者の権利をも守ることができるようになる。

発明を実施するための最良の形態

以下、この発明の実施の形態によるデータ配信システムおよび記録装置を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

なお、以下では携帯電話網を介してデジタル音楽データを各携帯電話ユーザに

配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、たとえば画像データ、映像データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

（実施の形態１）

図１を参照して、著作権の存在する音楽情報を管理するライセンスサーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機およびメモリカードが正規の機器であるか否かの認証を行なう。

配信キャリア２０は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ１０に中継する。ライセンスサーバ１０は、配信リクエストがあると、認証サーバ１２により携帯電話ユーザの携帯電話機およびメモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア２０の携帯電話網を介して、各携帯電話ユーザの携帯電話機に対してコンテンツデータを配信する。

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

さらに、たとえば携帯電話ユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

以下では、このようなライセンスサーバ１０と認証サーバ１２と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを

伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有する携帯電話ユーザ２が自己の携帯電話機１０２により、配信サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等を携帯電話ユーザ２が直接配信サーバ３０から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けている携帯電話ユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、携帯電話ユーザにとっての利便性が向上する。

図１に示すように、携帯電話ユーザ１が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、携帯電話ユーザ２に対してコピーさせる場合をコンテンツデータの「複製」と呼ぶ。

この場合に、携帯電話機１００および１０２を介して、メモリカード１１０と１１２との間で暗号化されたコンテンツデータ（音楽データ）および再生のために必要な情報（再生情報）が複製される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護にかかわる情報であるライセンスＩＤやアク

セス再生に関する制限情報等とを有する。

このような構成とすることによって、一旦配信サーバ３０より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機１００および１０２がＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙ　Ｐｈｏｎｅ）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、携帯電話ユーザ１と携帯電話ユーザ２との間における情報の複製を行なうことが可能である。

図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するための復号鍵保護を実現する構成である。

本発明の実施の形態においては、特に、配信、再生および複製の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。また、再生回数の制限を設けた再生権の発行を可能とし、利用者にとって利便性が高く、かつ著作権に対して十分なセキュリティー強度を維持できる構成を説明する。

次に図２を用いて、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する。

まず、配信サーバより配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンスキーＫｃで復号可能な暗号化が施される。ライセンスキーＫｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したデータであることを示すものとする。

さらに、配信サーバからは、暗号化コンテンツデータとともに、コンテンツデータに関するあるいはサーバへのアクセスに関する平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、ライセンスとしては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１および再生回路における制御情報である再生回路制御情報ＡＣ２等が存在する。

後ほど詳細に説明するが、再生回路制御情報ＡＣ２は、再生回数の制限や複製（移動）可能なライセンス数を示す情報を含み、メモリカード内において情報の管理および更新が実行される。

図３には、図１に示したデータ配信システムにおいて使用されるキーデータ（鍵データ）等の特性が示される。

図３を参照して、コンテンツ再生回路（携帯電話機）およびメモリカードには固有の公開暗号鍵ＫＰｐ（ｎ）およびＫＰｍｃ（ｍ）がそれぞれ設けられ、公開暗号鍵ＫＰｐ（ｎ）およびＫＰｍｃ（ｍ）はコンテンツ再生回路（携帯電話機）のクラス固有の秘密復号鍵Ｋｐ（ｎ）およびメモリカードのクラス固有の秘密復号鍵Ｋｍｃ（ｍ）によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードのクラスごとに異なる値を持つ。

また、メモリカードおよび再生回路のクラス証明書として、Ｃｐ（ｎ）およびＣｍｃ（ｍ）がそれぞれ設けられる。ここで、自然数ｍはメモリカードの、自然数ｎはコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。

これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、｛ＫＰｍｃ（ｍ）／／Ｃｍｃ（ｍ）｝ＫＰｍａおよび｛ＫＰｐ（ｎ）／／Ｃｐ（ｎ）｝ＫＰｍａの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で

共通の認証鍵である。認証鍵ＫＰｍａを用いて認証データを復号すると、その復号結果から認証データの正当性が確認できる。言い換えれば、認証鍵ＫＰｍａは、クラス固有の公開暗号鍵およびその証明書であるクラス証明書を承認するために用いられる鍵である。なお、認証データを作成するための暗号化は、認証鍵と対をなす非対称な秘密鍵によって行なわれる。

メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、再生および複製が行なわれるごとにサーバ３０、携帯電話機１００または１０２、メモリカード１１０または１１２において生成される共通鍵Ｋｓ１～Ｋｓ４が用いられる。

ここで、共通鍵Ｋｓ１～Ｋｓ４は、サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ４を「セッションキー」とも呼ぶこととする。

これらのセッションキーＫｓ１～Ｋｓ４は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび複製（受信側）セッションごとに発生し、セッションキーＫｓ３は、同様にメモリカードにおいて再生セッションおよび複製（送信側）セッションごとに発生する。セッションキーＫｓ４は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

また、メモリカード１００内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される暗号鍵ＫＰｍ（ｉ）（ｉ：自然数）と、暗号鍵ＫＰｍ（ｉ）で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍ（ｉ）が存在する。ここで、自然数ｉは、各メモリカードを区別するための番号を表わす。

その他の鍵としては、再生回路に共通の秘密鍵として、主としてライセンスキーＫｃの取得に利用される共通鍵方式における秘密鍵Ｋｃｏｍが存在する。秘密鍵Ｋｃｏｍは、配信サーバおよび携帯電話機の双方において保持され、ライセンスキーＫｃ等の暗号化および取得のための復号処理にそれぞれ使用される。

なお、共通鍵Ｋｃｏｍを、公開鍵方式における公開暗号鍵ＫＰｃｏｍおよび秘密復号鍵Ｋｃｏｍの組に置き換えて運用することも可能である。この場合には、公開暗号鍵ＫＰｃｏｍは配信サーバに保持されてライセンスキーＫｃの暗号化に使用され、秘密復号鍵Ｋｃｏｍは、携帯電話機に保持されてライセンスキーＫｃの取得に使用される。

図４を参照して、ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃ（ｍ）／／Ｃｍｃ（ｍ）｝ＫＰｍａおよび｛ＫＰｐ（ｎ）／／Ｃｐ（ｎ）｝ＫＰｍａを通信装置３５０およびデータバスＢＳ１を介して受けて、認証鍵ＫＰｍａによる復号処理を行なう復号処理部３１２とを含む。

データ処理部３１０は、さらに、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃ（ｍ）を用いて暗号化して、データバスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをデータバスＢＳ１をより受けて、復号処理を行なう復号処理部３２０と、再生回路

に共通な秘密鍵Ｋｃｏｍを保持するＫｃｏｍ保持部３２２とを含む。

データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンスキーＫｃおよび再生回路制御情報ＡＣ２を再生回路共通の秘密鍵Ｋｃｏｍで暗号化する暗号化処理部３２４と、暗号化処理部３２４から出力されたデータを復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍ（ｉ）によって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してデータバスＢＳ１に出力するための暗号化処理部３２８とを含む。

なお、共通鍵方式における秘密復号Ｋｃｏｍに代えて、公開鍵方式における公開暗号鍵ＫＰｃｏｍおよび秘密復号鍵Ｋｃｏｍの組を用いる場合には、Ｋｃｏｍ保持部３２２に相当する部分に公開暗号鍵ＫＰｃｏｍが保持される。さらに、暗号化処理部３２４によって、公開暗号鍵ＫＰｃｏｍによる暗号化が行なわれる。

ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図５を参照して、携帯電話機１００においては、携帯電話機のクラスを表わす自然数ｎ＝１、携帯電話機を個別に識別する自然数ｉ＝１とする。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ

１１２０に与え得る信号に変換するための外部インタフェース部１１２２とを含む。

携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と、携帯電話機のクラスごとにそれぞれ設定される公開暗号鍵ＫＰｐ（１）およびクラス証明書Ｃｐ（１）を公開復号鍵ＫＰｍａで復号可能な状態に暗号化したデータを保持する認証データ保持部１５００を含む。

携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ（１）を保持するＫｐ保持部１５０２と、データバスＢＳ２から受けたデータをＫｐ（１）によって復号しメモリカードによって発生されたセッションキーＫｓ３を得る復号処理部１５０４と、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でデータバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ４を乱数等により発生するセッションキー発生部１５０８と、生成されたセッションキーＫｓ４を復号処理部１５０４によって得られたセッションキーＫｓ３によって暗号化しデータバスＢＳ２に出力する暗号化処理部１５０６と、データバスＢＳ２上のデータをセッションキーＫｓ４によって復号して出力する復号処理部１５１０とを含む。

携帯電話機１００は、さらに、再生回路に共通に設定される秘密鍵Ｋｃｏｍを保持するＫｃｏｍ保持部１５１２と、復号処理部１５１０が出力する｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍを秘密鍵Ｋｃｏｍで復号しライセンスキーＫｃおよび再生回路制御情報ＡＣ２を出力する復号処理部１５１４と、データバスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１５１４より取得してライセンスキーＫｃによって復号しコンテンツデータを出力する復号処理部１５１６とを含む。携帯電話機１００は、さらに、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８と音声再生部１１１２の出力を受けて、動作モードに応じて選択的に出力する

ための切換部１５２５と、切換部１５２５の出力を受けて、ヘッドホン１３０と接続するための接続端子１５３０とを含む。

なお、共通鍵Ｋｃｏｍに代えて公開鍵方式における公開暗号鍵ＫＰｃｏｍおよび秘密復号鍵Ｋｃｏｍの組を用いる場合には、Ｋｃｏｍ保持部１５１２に相当する部分に秘密復号鍵Ｋｃｏｍが保持される。さらに、復号処理部１５１４によって、秘密復号鍵Ｋｃｏｍによる復号が行なわれる。

また、図５においては、説明の簡素化のため、携帯電話機のうち本発明のコンテンツデータの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。

図５に記載されたブロックのうち、アンテナ１１０２，送受信部１１０４、コントローラ１１０６，キー１１０８、ディスプレイ１１１０、音声再生部１１１２、コネクタ１１２０、外部インタフェース１１２２、切換部１５２５および接続端子１５３０の、通話処理に関するあるいは通話処理と共用されるブロック群除いた部分が、コンテンツデータの配信および再生に関するコンテンツ再生部に相当する。なお、携帯電話ユーザの利便性を図るために、携帯電話機１００のうちのコンテンツ再生部に相当するブロック群を、音楽再生モジュールとして着脱可能なモジュール化する構成を採用することも可能である。

携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図６を参照して、既に説明したように、公開暗号鍵ＫＰｍ（ｉ）およびこれに対応する秘密復号鍵Ｋｍ（ｉ）は、メモリカードごとに固有の値であるが、メモリカード１１０においては、この自然数ｉ＝１として取扱う。また、メモリカードの固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃ（ｍ）およびＫｍｃ（ｍ）が設けられ、メモリカードのクラス証明書としてＣｍｃ（ｍ）が設けられるが、メモリカード１１０においては、これらは自然数ｍ＝１でそれぞれ表わされるものとする。

メモリカード１１０は、認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ（１）を保持するＫｍｃ保持部１４０２と、メモ

リカードごとに固有に設定される秘密復号鍵Ｋｍ（１）を保持するＫｍ（１）保持部１４２１と、Ｋｍ（１）によって復号可能な公開暗号鍵ＫＰｍ（１）を保持するＫＰｍ（１）保持部１４１６とを含む。認証データ保持部１４００は、メモリカード１１０に対応して設定される公開暗号鍵ＫＰｍｃ（１）を認証鍵ＫＰｍａで復号することで認証可能な状態に暗号化して保持する。

このように、メモリカードという記録装置の公開暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ（１）をＫｍｃ（１）保持部１４０２から受けて配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ１、または他のメモリカードが複製セッションにおいて生成したセッションキーＫｓ３を接点Ｐａに出力する復号処理部１４０４とを含む。

メモリカード１１０は、さらに、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、データバスＢＳ３に与えられるデータから認証鍵ＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してデータバスＢＳ３に出力する暗号化処理部１４０６とを含む。

メモリカード１１０は、さらに、配信、再生および複製の各セッションにおいてセッションキーを発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ３を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐ（ｎ）もしくはＫＰｍｃ（ｍ）によって暗号化してデータバスＢＳ３に送出する暗号化処理部１４１０と、ＢＳ３よりセッションキーＫｓ３によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ３によって復号し、復号結果をにデータバスＢＳ４に送出する復号処理部１４１２とを含む。

メモリカード１１０は、さらに、「複製」時にデータバスＢＳ４上のデータを他のメモリカードの公開暗号鍵ＫＰｍ（ｉ）（ｉ≠１）で暗号化する暗号化処理部１４２４と、データバスＢＳ４上のデータを公開暗号鍵ＫＰｍ（１）と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ（１）によって復号するための復号処理部１４２２と、公開暗号鍵ＫＰｍ（１）で暗号化されている、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２をデータバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをデータバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。

メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を保持するためのライセンス情報保持部１４４０と、データバスＢＳ３を介して外部との間でデータ授受を行ない、データバスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。ライセンス情報保持部１４４０は、データバスＢＳ４との間でライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のデータの授受が可能である。

図７を参照して、ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンス情報である、ライセンスＩＤ、データコンテンツＩＤデータおよびアクセス制限情報ＡＣ１をバンクごとに保持する。

図８を参照して、アクセス制限情報ＡＣ１は、再生回数制限情報Ｓｕｂ＿Ｐｌａｙと、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅとを含む。図８においては、再生回数制限情報Ｓｕｂ＿Ｐｌａｙは、一例として８ビットのデータである。Ｓｕｂ＿Ｐｌａｙの値がＦＦ（ｈ）である場合には再生回数に制限がないことを示し、その値がＯ（ｈ）である場合には、もはや再生不能であることを示す。また、Ｓｕｂ＿Ｐｌａｙの値が１（ｈ）～７Ｆ（ｈ）の範囲である場合は、この値は再生可能な回数を示し、再生されるごとにＳｕｂ＿Ｐｌａｙの値は減じられる。なお、（ｈ）は、１６進数表示を意味する。

また、図８においては、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅは、一例として同様に８ビットのデータで示される。Ｓｕｂ＿Ｍｏｖｅの値がＦＦ（ｈ）である場

合には、複製が禁止されていることを示す。また、Ｓｕｂ＿Ｍｏｖｅの値がＯ（ｈ）～７Ｆ（ｈ）の範囲である場合は、この値は所有ライセンス数を示し、他のメモリカードに複製させるごとに、複製したライセンス数に応じてＳｕｂ＿Ｍｏｖｅの値は減じられ、その値がＯ（ｈ）となった場合には、もはや複製するライセンスが無いことを示す。

アクセス制限情報ＡＣ１は、ライセンス購入時に利用者側からの指定に応じて生成されるライセンス購入条件ＡＣに応じて、配信動作時に配信サーバ３０によって発行され、再生および複製動作が実行されるごとに、メモリカード１１０内において、更新および保持される。

なお、図６において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般には、内部解析や改ざんを物理的および論理的に防衛する技術を用いた、外部から直接アクセス不可能なタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）である。

もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図６に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタントモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

次に、本発明の実施の形態に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

まず、図９および図１０のフローチャートを用いて、実施の形態１に従うデータ配信システムにおけるコンテンツの購入時に発生する配信セッション時の動作（以下、配信動作ともいう）を説明する。

図９および図１０においては、携帯電話ユーザ１が、メモリカード１１０を用

いることで、携帯電話機１００を介して配信サーバ３０から音楽データであるコンテンツデータの配信を受ける場合の動作が説明される。

図９を参照して、まず、携帯電話ユーザ１の携帯電話機１００から携帯電話ユーザによりタッチキー部１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａが出力される（ステップＳ１０２）。

携帯電話機１００は、メモリカード１１０から受理した認証のための認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａに加えて、コンテンツ再生回路の認証のための認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａと、コンテンツＩＤ、ライセンス購入条件データＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａ、｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａ、｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａ、ライセンス購入条件ＡＣを受信し（ステップＳ１０６）、復号処理部３１２において認証鍵ＫＰｍａで復号処理を実行して、メモリカード１１０の公開暗号鍵およびクラス証明書であるＫＰｍｃ（１）およびＣｍｃ（１）と、携帯電話機１００のコンテンツ再生回路の公開暗号鍵およびクラス証明書であるＫＰｐ（１）およびＣｐ（１）を受理する（ステップＳ１０８）。

配信制御部３１５は、受理したクラス証明データＣｍｃ（１）およびＣｐ（１）に基づいて、認証サーバ１２に対して照会を行ない、これらのクラス証明書が有効であれば正規の機器であり、これらの公開暗号鍵が有効であることが確認される。公開暗号鍵が有効である場合には次の処理（ステップＳ１１２）に移行し、これらの公開暗号鍵が無効である場合には、処理を終了（ステップＳ１６０）する（ステップＳ１１０）。

なお、認証データ｛ＫＰｍｃ（１）｝ＫＰｍａおよび認証データ｛ＫＰｐ（１）｝ＫＰｍａは、それぞれが認証鍵ＫＰｍａによって復号することで、その正当

性が判断可能な暗号化が施されているため、認証サーバ１２に対して照会を行なわず、ライセンスサーバ１０の配信制御部３１５が、認証鍵ＫＰｍａによる復号結果から独自に認証を行なう構成とすることもできる。

照会の結果、正規のクラス証明書を持つメモリカードと再生回路とを備える携帯電話機からのアクセスであることが確認されると、配信サーバ３０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ（１）によって、暗号化処理部３１８によって暗号化される（ステップＳ１１２）。

暗号化されたセッションキーＫｓ１は、｛Ｋｓ１｝Ｋｍｃ（１）として、データバスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１４）。

携帯電話機１００が、暗号化されたセッションキー｛Ｋｓ１｝Ｋｍｃ（１）を受信すると（ステップＳ１１６）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ（１）により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１１８）。

コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカードにおいて配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２および公開暗号鍵ＫＰｍ（１）を１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ（１）｝Ｋｓ１をデータバスＢＳ３に出力する（ステップＳ１２０）。

データバスＢＳ３に出力された暗号データ｛Ｋｓ２／／ＫＰｍ（１）｝Ｋｓ１は、データバスＢＳ３から端子１２０２およびメモリインタフェース１２００を

介して携帯電話機１００に送信され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２２）。

配信サーバ３０は、暗号化データ｛Ｋｓ２／／ＫＰｍ（１）｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫＳ２およびメモリカード１１０固有の公開暗号鍵ＫＰｍ（１）を受理する（ステップＳ１２４）。

配信制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件ＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生回路制御情報ＡＣ２を生成する（ステップＳ１２６）。さらに、暗号化コンテンツデータを復号するためのライセンスキーＫｃを情報データベース３０４より取得する（ステップＳ１２８）。

図１０を参照して、配信制御部３１５は、取得したライセンスキーＫｃおよび再生回路制御情報ＡＣ２を暗号化処理部３２４に与える。暗号化処理部３２４は、Ｋｃｏｍ保持部３２２より得られる、再生回路共通の秘密鍵Ｋｃｏｍによって、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２を暗号化する（ステップＳ１３０）。

暗号化処理部３２４が出力する暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍと、配信制御部３１５が出力するライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１とは、暗号化処理部３２６によって、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ（１）によって暗号化される（ステップＳ１３２）。暗号化処理部３２８は、暗号化処理部３２６の出力を受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、データバスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３４）。

このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを

向上させることができる。

携帯電話機１００は、送信された暗号化データ｛｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）｝Ｋｓ２を受信し（ステップＳ１３６）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを復号化処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてデータバスＢＳ３の受信データを復号しデータバスＢＳ４に出力する（ステップＳ１３８）。

この段階で、データバスＢＳ４には、Ｋｍ（１）保持部１４２１に保持される秘密復号鍵Ｋｍ（１）で復号可能な｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）が出力される。コントローラ１４２０の指示によって、｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）は、メモリ１４１５に記録される（ステップＳ１４０）。一方、｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）は、復号処理部１４２２において、秘密復号鍵Ｋｍ（１）によって復号され、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１のみが受理される（ステップＳ１４２）。

ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１については、ライセンス情報保持部１４４０に記録される（ステップＳ１４４）。

ステップＳ１４４までの処理がメモリ回路で正常に終了した段階で、携帯電話機１００から配信サーバ３０にコンテンツデータの配信要求がなされる（ステップＳ１４６）。

配信サーバ３０は、コンテンツデータの配信要求を受けて、情報データベース３０４より、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをデータバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１４８）。

携帯電話機１００は、｛Ｄａｔａ｝Ｋｃ／／Ｄａｔａ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄａｔａ｝ＫｃおよびＤａｔａ－ｉｎｆを受理する（ステップＳ１５０）。暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄ

ａｔａ－ｉｎｆはメモリインタフェース１２００および端子１２０２を介してメモリカード１１０のデータバスＢＳ３に伝達される。メモリカード１１０においては、受信した｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１５２）。

さらに、メモリカード１１０から配信サーバ３０へは、配信受理の通知が送信され（ステップＳ１５４）、配信サーバ３０で配信受理を受信すると（ステップＳ１５６）、課金データベース３０２への課金データの格納等を伴って、配信終了の処理が実行され（ステップＳ１５８）、全体の処理が終了する（ステップＳ１６０）。

このようにして、携帯電話機１００のコンテンツ再生部およびメモリカード１１０が正規の機器であること、同時に、それぞれがクラス証明書Ｃｐ（１）およびＣｍｃ（１）とともに暗号化して送信できた公開暗号鍵Ｋｐ（１）およびＫｍｃ（１）が有効であることを確認した上で、コンテンツデータを配信することができ、十分なセキュリティー強度を確保することができる。

次に、図１１のフローチャートを用いて、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから音楽を再生し、外部に出力するための再生セッション時の動作（以下、再生動作ともいう）を説明する。

図１１を参照して、携帯電話機１００のタッチキー部１１０８等からの携帯電話ユーザ１の指示により、再生リクエストが生成される（ステップＳ２００）。携帯電話機１００は、再生リクエストの生成に応じて、認証データ保持部１５００より、認証鍵ＫＰｍａで復号することで認証可能な認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａをデータバスＢＳ２に出力する（ステップＳ２０２）。

認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａは、データバスＢＳ２およびメモリインタフェース１２００を介してメモリカード１１０に伝達される。

メモリカード１１０においては、端子１２０２を介してデータバスＢＳ３に伝達される認証のための暗号化データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａは、復号処理部１４０８に取込まれる。復号処理部１４０８は、ＫＰｍａ保持部１

４１４から認証鍵ＫＰｍａを受けて、データバスＢＳ３のデータを復号処理し、コンテンツ再生部すなわち携帯電話機１００の種類に固有の公開暗号鍵ＫＰｐ（１）およびクラス証明書Ｃｐ（１）を得る。コントローラ１４２０は、データバスＢＳ３を介して公開暗号鍵ＫＰｐ（１）およびクラス証明書Ｃｐ（１）を受理する（ステップＳ２０４）。

コントローラ１４２０は、復号処理部１４０８の復号結果に基づいて、受理した携帯電話機１００のコンテンツ再生回路の認証作業を行ない、携帯電話機１００のコンテンツ再生回路が承認されたものである場合には処理を次のステップ（ステップＳ２０８）に進める（ステップＳ２０６）。一方、携帯電話機１００のコンテンツ再生回路が非承認である場合には、再生セッションの処理を終了する（ステップＳ２４０）。

次に、コントローラ１４２０は、セッションキー発生部１４１８に、再生セッションにおけるセッションキーＫｓ３の生成をデータバスＢＳ４を介して指示する。セッションキー発生部１４１８によって生成されたセッションキーＫｓ３は、暗号化処理部１４１０に送られる。暗号化処理部１４１０は、復号処理部１４０８によって得られた携帯電話機１００の公開暗号鍵ＫＰｐ（１）によってセッションキーＫｓ３を暗号化しＫＰｐ（１）に対応する秘密復号鍵Ｋｐ（１）で復号可能な暗号化データ｛Ｋｓ３｝Ｋｐ（１）をデータバスＢＳ３に出力する（ステップＳ２０８）。

携帯電話機１００は、端子１２０２およびメモリインタフェース１２００を介して、データバスＢＳに暗号化データ｛Ｋｓ３｝Ｋｐ（１）を受ける。暗号化データ｛Ｋｓ３｝Ｋｐ（１）は、復号処理部１５０４によって復号され、メモリカード１１０で生成されたセッションキーＫｓ３が受理される（ステップＳ２１０）。

コントローラ１１０６は、セッションキーＫｓ３の受理に応じて、セッションキー発生部１５０８に対して、再生セッションにおいて携帯電話機１００で生成されるセッションキーＫｓ４の発生をデータバスＢＳ２を介して指示する。生成されたセッションキーＫｓ４は暗号化処理部１５０６に送られ、復号処理部１５０４によって得られたセッションキーＫｓ３によって暗号化された｛Ｋｓ４｝Ｋ

ｓ３がデータバスＢＳ２に受理される（ステップＳ２１２）。

暗号化されたセッションキー｛Ｋｓ４｝Ｋｓ３は、メモリインタフェース１２００を介してメモリカード１１０に伝達される。メモリカード１１０においては、データバスＢＳ３に伝達される暗号化されたセッションキー｛Ｋｓ４｝Ｋｓ３を復号処理部１４１２によって復号し、携帯電話機１００で生成されたセッションキーＫｓ４を受理する（ステップＳ２１４）。

セッションキーＫｓ４の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する。

コントローラ１４２０は、まず所有ライセンス数Ｓｕｂ＿Ｍｏｖｅを確認し、この値が０であるときは、すでにライセンスが無い状態であるので再生セッションを終了する（ステップＳ２４０）。一方、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅの値が０以外であるときには、処理を次のステップに進める（ステップＳ２１６）。

次のステップにおいては、コントローラ１４２０は、再生回数制限情報Ｓｕｂ＿Ｐｌａｙを確認し、この値が０であるときは、すでに再生不能の状態であるので再生セッションを終了する（ステップＳ２４０）。再生回数制限情報Ｓｕｂ＿Ｐｌａｙの値が１（ｈ）～７Ｆ（ｈ）である場合には、Ｓｕｂ＿Ｐｌａｙの値すなわち再生可能回数を１減じて（ステップＳ２２０）、再生セッションの処理を進める。一方、再生回数制限情報Ｓｕｂ＿Ｐｌａｙの値がＦＦ（ｈ）である場合には、当該ライセンスについては再生回数の制限がないことを意味するので、ステップＳ２２０を実行することなく再生セッションの処理が実行される（ステップＳ２１８）。

ステップＳ２１８において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーＫｃおよび再生回路制御情報ＡＣ２の復号処理が実行される。具体的には、コントローラ１４２０の指示に応じて、メモリ１４１５からデータバスＢＳ４に読出された暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）を復号処理部１４２２がメモリカード１１０固有の秘密復号鍵Ｋｍ（１）によって復号し、共通の秘密鍵Ｋｃｏｍによって復号

可能な暗号化データ｛Ｋｃ／／ＡＣ２｝ＫｃｏｍがデータバスＢＳ４上に得られる（ステップＳ２２２）。

得られた暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍは、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ４によってデータバスＢＳ４から受けた暗号化データをさらに暗号化し、｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ｝Ｋｓ４をデータバスＢＳ３に出力する（ステップＳ２２４）。

データバスＢＳ３に出力された暗号化データは、メモリインタフェース１２００を介して携帯電話機１００に送出される。

携帯電話機１００においては、メモリインタフェース１２００を介してデータバスＢＳ２に伝達される暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ｝Ｋｓ４を復号処理部１５１０によって復号処理を行ない、暗号化されたライセンスキーＫｃおよび再生回路制御情報ＡＣ２を受理する（ステップＳ２２６）。

復号処理部１５１４は、暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍを、Ｋｃｏｍ保持部１５１２から受けた再生回路に共通の秘密鍵Ｋｃｏｍによって復号し、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２を受理する（ステップＳ２２８）。復号処理部１５１４は、ライセンスキーＫｃを復号処理部１５１６に伝達し、再生回路制御情報ＡＣ２をデータバスＢＳ２に出力する。

コントローラ１１０６は、データバスＢＳ２を介して、再生回路制御情報ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２３０）。

ステップＳ２３０においては、再生回路制御情報ＡＣ２によって再生不可と判断される場合には、再生セッションは終了される（ステップＳ２４０）。一方、再生可能である場合には、メモリカード１１０よりメモリに記録されたリクエスト曲の暗号化されたコンテンツデータ｛Ｄａｔａ｝ＫｃがデータバスＢＳ３に出力され、メモリインタフェース１２００を介して携帯電話機１００に伝達される（ステップＳ２３２）。

携帯電話機１００においては、メモリカード２１０から出力されデータバスＢＳ２に伝達された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１５１

６においてライセンスキーＫｃによって復号し、平文化されたコンテンツデータＤａｔａを得ることができる（ステップＳ２３４）。復号された平文化コンテンツデータＤａｔａは音楽再生部１５１８によって音楽信号に変換され（ステップＳ２３６）、混合部１５２５および端子１５３０を介して外部に再生された音楽を出力することによって処理が終了する（ステップＳ２４０）。

このような構成とすることで、メモリカード１１０側において、コンテンツ再生回路である携帯電話機１００の認証を行なった上で、再生処理を禁止することが可能となる。また、メモリカード内で更新、保持されるアクセス制限情報を反映した再生動作を実行することができる。

再生セッションにおいても、携帯電話機１００およびメモリカード１１０でそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信する。この結果、配信セッションと同様に、再生セッションにおいてもデータのそれぞれの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティーを向上させることができる。

次に、図１２、図１３および図１４のフローチャートを用いて、２つのメモリカード間におけるコンテンツデータの複製セッション時の動作（以下、複製動作とも称する）を説明する。

図１２、図１３および図１４においては、２つのメモリカード１１０および１１２の間で携帯電話機１００および１０２を介した、コンテンツデータおよびキーデータ等の複製動作が説明される。

図１２、図１３および図１４においては、携帯電話機１００およびメモリカード１１０についての種類を識別するための自然数をｍ＝１およびｎ＝１とし、携帯電話機１０２およびメモリカード１１２についての種類を識別するため自然数をｍ＝２およびｎ＝２とする。また、メモリカード１１０および１１２を識別するための自然数ｉは、それぞれｉ＝１およびｉ＝２であるものとする。

携帯電話機１００およびメモリカード１１０が送信側であり、携帯電話機１０２およびメモリカード１１２が受信側であるものとする。また、携帯電話機１０２も、メモリカード１１０と同様の構成を有するメモリカード１１２が装着され

ているものとする。以下、メモリカード１１２の各構成部分については、メモリカード１１０の対応する部分と同一の符号を用いて説明する。

図１２を参照して、まず、送信側である携帯電話ユーザ１の携帯電話機１００から、携帯電話ユーザ１によりタッチキー部１１０８のキーボタンの操作等によって、コンテンツ複製リクエストがなされる。（ステップＳ３００）。

生成された複製リクエストは、受信側である携帯電話ユーザ２の携帯電話機１０２を介してメモリカード１１２に伝達される。メモリカード１１２においては、認証データ保持部１５００より、メモリカード１１２に対応する公開暗号鍵ＫＰｍｃ（２）およびクラス証明書Ｃｍｃ（２）が暗号化された認証データ｛ＫＰｍｃ（２）／／Ｃｍｃ（２）｝ＫＰｍａが出力される（ステップＳ３０２）。

メモリカード１１２の認証データ｛ＫＰｍｃ（２）／／Ｃｍｃ（２）｝ＫＰｍａは、携帯電話ユーザ２の携帯電話機１０２から送信され、携帯電話ユーザ１の携帯電話機１００を経由してメモリカード１１０に受信される（ステップＳ３０４）。

メモリカード１１０においては、復号処理部１４０８によって、メモリカード１１２の認証データが復号され、メモリカード１１２に関するクラス証明書Ｃｍｃ（２）および公開暗号鍵ＫＰｍｃ（２）が受理される（ステップＳ３０６）。コントローラ１４２０は、データバスＢＳ３を介して復号処理部１４０８の復号結果に基づいて、認証作業を実行する（ステップＳ３０８）。

コントローラ１４２０は、メモリカード１１２に関する認証データ｛ＫＰｍｃ（２）／／Ｃｍｃ（２）｝ＫＰｍａを認証鍵ＫＰｍａにて復号した復号結果から、認証データ｛ＫＰｍｃ（２）／／Ｃｍｃ（２）｝ＫＰｍａが正規のキーから出力された認証データであることを確認することができる。この確認を実行し、正規のキーから出力された有効な認証データである場合には、公開暗号鍵ＫＰｍｃ（２）およびクラス証明書Ｃｍｃ（２）を承認して、次のステップＳ３１０を実行する。一方、正規のキーから出力されたことが確認できない無効な認証データである場合においては、複製セッションを終了する（ステップＳ３７０）。

この場合においては、コントローラ１４２０は、セッションキー発生部１４１８に対して、複製セッション時に送信側で発生されるセッションキーＫｓ３の出

力を指示する。セッションキーへ発生部１４１８によって生成されたセッションキーＫｓ３は、暗号化処理部１４１０に伝達される。

暗号化処理部１４１０は、さらに、ステップＳ３０６において復号処理部１４０８によって復号されたメモリカード１１２の公開暗号鍵ＫＰｍｃ（２）を受けて、ＫＰｍｃ（２）によってセッションキーＫｓ３を暗号化する。これにより、暗号化されたセッションキー｛Ｋｓ３｝Ｋｍｃ（２）がデータバスＢＳ３に出力される（ステップＳ３１２）。データバスＢＳ３に出力された｛Ｋｓ３｝Ｋｍｃ（２）は、携帯電話機１００および携帯電話機１０２を介してメモリカード１１２に伝達される。

メモリカード１１２は、メモリカード１１０から出力された｛Ｋｓ３｝Ｋｍｃ（２）を受けて、復号処理部１４０４によってメモリカード１１２に対応する秘密復号鍵Ｋｍｃ（２）による復号処理を実行し、送信側のメモリカード１１０によって生成されたセッションキーＫｓ３を受理する（ステップＳ３１４）。

メモリカード１１２のコントローラ１４２０は、セッションキーＫｓ３の受理に応じて、セッションキー発生部１４１８に対して、複製セッションにおいて受信側で発生されるべきセッションキーＫｓ２の生成を指示する。生成されたセッションキーＫｓ２は、切換スイッチ１４４６中の接点Ｐｆおよび切換スイッチ１４４４中の接点Ｐｃを経由して暗号化処理部１４０６に伝達される。

暗号化処理部１４０６は、復号処理部１４０４からステップＳ３１６で得られたセッションキーＫｓ３を受けて、切換スイッチ１４４４の接点Ｐｃと切換スイッチ１４４６の接点の切換によって得られるセッションキーＫｓ２と公開暗号鍵ＫＰｍ（２）をセッションキーＫｓ１によって暗号化し、｛Ｋｓ２／／ＫＰｍ（２）｝Ｋｓ３をデータバスＢＳ３に出力する（ステップＳ３１６）。データバスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ（２）｝は、携帯電話機１０２および１００を介してメモリカード１１０のデータバスＢＳ３に伝達される。

メモリカード１１０においては、データバスＢＳ３に伝達された暗号化データを復号処理部１４１２によってセッションキーＫｓ３を用いて復号し、メモリカード１１２に関するセッションキーＫｓ２および公開暗号鍵ＫＰｍ（２）を受理

する（ステップＳ３１８）。

次に、図１３を参照して、メモリカード１１０のコントローラ１４２０は、セッションキーＫｓ２および公開暗号鍵ＫＰｍ（２）の受理に応じて、ライセンス情報保持部１４４０内のアクセス制限情報ＡＣ１の確認を実行する。

まず、ライセンス情報保持部１４４０内に格納された対応する再生回数制限情報Ｓｕｂ＿Ｐｌａｙを確認し、この値が０であるときは、すでに対応するライセンスは、再生不能の状態であるので複製セッションを終了する（ステップＳ３７０）。一方、再生回数制限情報Ｓｕｂ＿Ｐｌａｙの値が０でない場合には、複製セッションの処理が進められる（ステップＳ３２０）。

次に、コントローラ１４２０は、ライセンス情報保持部１４４０内に格納された対応する所有ライセンス数Ｓｕｂ＿Ｍｏｖｅを確認し、この値が０もしくはＦＦ（ｈ）であるときは、すでにライセンスが無い状態もしくは、ライセンスが当初から複製禁止の状態であるので複製セッションを終了する（ステップＳ３７０）。一方、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅの値が０およびＦＦ（ｈ）０以外であるときには、処理を次のステップに進める（ステップＳ３２２）。

次のステップにおいては、コントローラ１４２０は、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅの更新を実行する。ステップＳ３２４において、複製ライセンス数の入力指示が実行され、残りライセンス数の全てについて複製を指示した場合（ステップＳ３２６）には、コントローラ１４２０は、ライセンス情報保持部１４４０からアクセス制限情報ＡＣ１を取得して、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅの値を０に更新する（ステップＳ３２８）。

また、ステップＳ３２４において指示された複製ライセンス数が残りライセンス数よりも小さい場合には（ステップＳ３２６）、コントローラ１４２０は、ライセンス情報保持部１４４０からアクセス制限情報ＡＣ１を取得して、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅの値から、入力された複製ライセンス数を減算し、ライセンス情報保持部１４４０内のアクセス制限情報ＡＣ１を更新する（ステップＳ３３０）。所有ライセンス数Ｓｕｂ＿Ｍｏｖｅ＝０となると、以降の再生および複製が禁止される。

コントローラ１４２０は、所有ライセンス数Ｓｕｂ＿Ｍｏｖｅを更新した後、

ライセンス情報保持部１４４０より対応するコンテンツＩＤおよびライセンスＩＤを取得する（ステップＳ３３２）。

さらに、コントローラ１４２０は、複製するコンテンツデータに対応したセッションキーＫｃおよび再生情報に関する暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）の出力をメモリ１４１５に対して指示する。メモリ１４１５から出力された暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）は、復号処理部１４２２によって復号化され、｛Ｋｃ／／ＡＣ２｝ＫｃｏｍがデータバスＢＳ４上に得られる（ステップＳ３３４）。

ステップＳ３３２でライセンス情報保持部１４４０から取得されたライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１と、ステップＳ３３４で得られた｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍは、データバスＢＳ４から暗号化処理部１４２４に取込まれて暗号化される。暗号化処理部１４２４は、ステップＳ３２０において復号処理部１４１２で得られたメモリカード１１２固有の公開暗号鍵ＫＰｍ（２）によって、これらのデータを暗号化し、｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）を出力する（ステップＳ３３６）。

データバスＢＳ４に出力された暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）は、切換スイッチ１４４４中の接点Ｐｄを介して暗号化処理部１４０６に伝達される。暗号化処理部１４０６は、復号処理部１４１２によって得られたメモリカード１１２の生成したセッションキーＫｓ２を切換スイッチ１４４２の接点Ｐｂを介して受けて、接点Ｐｄより受けたデータをセッションキーＫｓ２によって暗号化する。

暗号化処理部１４０６は、｛｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）｝Ｋｓ２をデータバスＢＳ３に出力する（ステップＳ３３８）。ステップＳ３３８においてデータバスＢＳ３に出力された暗号化データは、携帯電話機１００および１０２を介して、複製セッションの受信側であるメモリカード１１２に伝達される。

次に、図１４を参照して、メモリカード１１２においては、復号処理部１４１

２においてセッションキー発生部１４１８によって生成されたセッションキーＫｓ２による復号が実行され、｛｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）が受理される（ステップＳ３４０）。

公開暗号鍵ＫＰｍ（２）で暗号化された｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）は、メモリ１４１５に記録される（ステップＳ３４２）。さらに、復号処理部１４２２において、メモリカード１１２に固有の秘密復号鍵Ｋｍ（２）による復号処理を実行することにより、ライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１が受理される（ステップＳ３４４）。

復号処理部１４２２によって得られたライセンスＩＤ、およびコンテンツＩＤおよびアクセス制限情報ＡＣ１は、データバスＢＳ４を介してライセンス情報保持部１４４０に記録される（ステップＳ３４６）。

このようにして、ステップＳ３３８までの処理が正常に終了することによって、再生情報が複製されたことに応答して、携帯電話機１０２を介してコンテンツデータの複製要求がさらに行なわれる（ステップＳ３４８）。

コンテンツデータの複製要求は携帯電話機１００を経由してメモリカード１１０に伝達され、これに応答して、メモリカード１１０中のメモリ１４１５より対応する暗号化コンテンツデータの｛Ｄａｔａ｝Ｋｃと付加情報Ｄａｔａ－ｉｎｆとがデータバスＢＳ３に出力される（ステップＳ３５０）。

データバスＢＳ３に出力されたこれらのデータは、携帯電話機１００および携帯電話機１０２を介してメモリカード１１２に入力され、メモリカード１１２中のメモリ１４１５に記録される（ステップＳ３５２）。

暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆの記録が終了すると、携帯電話機１０２を介して複製受理が送信される（ステップＳ３５４）。

これにより、メモリカード１１２および対応する携帯電話機１０２において正常に再生セッションが実行されれば、携帯電話機１０２によって、メモリカード１１２に記録された暗号化コンテンツデータを再生して音楽を聴取することが可

能となる。

送信側の携帯電話機１００においては、携帯電話機１０２から送信された複製受理を受信して（ステップＳ３５６）する。

複製受理を受信すると、メモリカード１１０においては、ライセンス情報保持部１４４０内の所有ライセンス数Ｓｕｂ＿Ｍｏｖｅを確認し（ステップＳ３５８）、この値が０である場合、すなわちライセンスが無くなった場合においては、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆの消去もしくは保持のいずれかをタッチキー部１１０８から入力することを要求する（ステップＳ３６０）。

したがって、ライセンスの無くなったコンテンツデータを消去したい場合には、タッチキー部１１０８より消去を指示することにより（ステップＳ３６２）、メモリカード１１０内のメモリ１４１５において、対応する暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、付加情報Ｄａｔａ－ｉｎｆを消去することができる（ステップＳ３６４）。なお、ライセンス情報保持部１４４０内に記録された対応するコンテンツＩＤ等の再生情報は、ステップＳ３２８にてアクセス制限情報ＡＣ１内のＳｕｂ＿Ｍｏｖｅが更新され、Ｓｕｂ＿Ｍｏｖｅ＝０となっているため、以降の再生セッションおよび複製セッションは禁止されている。

一方、コンテンツデータ等の保持が指示された場合および、ライセンス情報保持部中の所有ライセンス数Ｓｕｂ＿Ｍｏｖｅが０以外である場合（すなわち、ライセンスが残っている場合）においては、ステップＳ３６４はスキップされ、複製処理はこの段階で終了する（ステップＳ３６６）。

正常に複製セッションが行なわれた場合の複製処理終了ステップＳ３６６、もしくは認証チェック等によって複製セッションが中止された場合にはステップＳ３０８、Ｓ３２０およびＳ３２２からスキップされて複製セッション全体の処理が終了する（Ｓ３７０）。

このような構成とすることにより、複製セッションにおいても、受信回路側のコンテンツ再生回路（携帯電話機）およびメモリカードの認証を事前にチェックした後に、ライセンスキーや暗号化コンテンツデータの複製を実行する構成とするので、認証されていない再生回路（携帯電話機）もしくはメモリカードに対す

るコンテンツデータの複製の禁止を行なうことができる。

また、複製動作におけるライセンスの変化をメモリカード内で保持されるアクセス制限情報ＡＣ１（Ｓｕｂ＿Ｍｏｖｅ）にメモリカードが独自に反映させる構造になっている。したがって、再生情報および暗号化コンテンツデータを無制限に複製することを防止できる。

なお、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリ１４１５に記録された状態から、新たに配信サーバ３０をアクセスし、再生情報のみの配信のみを受けることが可能な配信サービスが考えられる。このように、再生情報のみの配信を受ければ、再び、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを再生して、音楽を聴取できるようになる。

再生情報のみの配信処理は、フローチャートには図示されていないが、配信セッションにおける図９および図１０において、暗号化コンテンツデータの授受に関する、ステップＳ１４６，Ｓ１４８，Ｓ１５０およびＳ１５２を実行しない処理に相当するため、ここでは詳細な説明を繰り返さない。

また、ステップＳ３２８において、複製を目的としてライセンス情報保持部１４４０内の再生情報を取得すると、アクセス制限情報ＡＣ１内のＳｕｂ＿Ｍｏｖｅの値を０に更新すると説明したが、当該データをライセンス情報保持部１４４０から消去しても同様の効果が得られる。

以上説明したように、実施の形態１に従う情報配信システムによれば、所有ライセンス数および再生可能回数といったアクセス制限情報を、配信サーバを介さずにメモリカード内のＴＲＭ領域で保持更新することができる。この結果、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができるので、コンテンツデータに対する著作権保護をより強固なものとすることができる。

（実施の形態２）

実施の形態２のデータ配信システムにおいては、実施の形態１のデータ配信システムの構成と異なって、再生回路共通の秘密鍵Ｋｃｏｍによって復号可能な暗号化を行なわない点を特徴とする。

すなわち、実施の形態２のデータ配信システムは、実施の形態１のデータ配信

システムが具備する配信サーバ３０内のライセンスサーバ１０に代えてライセンスサーバ１１を備える点で異なる。また、実施の形態２のデータ配信システムにおける携帯電話機の構成は、図５で説明した携帯電話機１００の構成に代えて携帯電話機１０１の構成が採用される。

図１５を参照して、ライセンスサーバ１１は、ライセンスサーバ１０と比較して、再生回路共通の秘密鍵Ｋｃｏｍ保持部３２２と、秘密鍵Ｋｃｏｍによる暗号化処理部３２４を具備しない点で異なる。すなわち、ライセンスサーバ１１においては、配信制御部３１５が出力するライセンスキーＫｃおよび再生回路制御情報ＡＣ２は、直接暗号化処理部３２６に伝達される。その他の回路構成および動作については図４に示すライセンスサーバ１０と同様であるので説明は繰返さない。

以降、ライセンスサーバ１１、認証サーバ１２および配信キャリア２０を合わせて配信サーバ３１と総称することとする。

図１６を参照して、実施の形態２に従うデータ配信システムにおいて使用される携帯電話機携帯電話機１０１は、実施の形態１で説明した携帯電話機１００の構成と比較して、再生回路共通の秘密鍵Ｋｃｏｍを保持するＫｃｏｍ保持部１５１２と秘密鍵Ｋｃｏｍによる復号処理部１５１４を具備しない点で異なる。

すなわち、携帯電話機１０１においては、配信サーバ３１において秘密鍵Ｋｃｏｍによる暗号化処理が施されていないことに対応して、セッションキーＫｓ４による復号処理を実行する復号処理部１５１０によって直接ライセンスキーＫｃが得られるため、これを復号処理部１５１０に直接与える構成となる。その他の回路構成および動作については携帯電話機１００の場合と同様であるので説明は繰返さない。

また、実施の形態２に従うデータ配信システムにおいて使用されるメモリカードについては、図６に示すメモリカード１１０と同一の構成であるので説明は繰返さない。

次に、再生回路共通の秘密鍵Ｋｃｏｍによる暗号化を省略することによる、配信、再生および複製の各セッションにおける動作の差異についてフローチャートで説明する。

次に。図１７のフローチャートを用いて、実施の形態２に従うデータ配信システムにおける配信動作を説明する。図１７においては、図９および図１０で示した実施の形態１に従うデータ配信システムにおける配信動作のフローチャートと異なる点について説明する。

図１７においては、携帯電話ユーザが、メモリカード１１０を用いることで、実施の形態２に従う配信サーバ３１から、携帯電話機１０１を介して音楽データであるコンテンツデータの配信を受ける場合の動作が説明される。

図１７を参照して、実施の形態２に従う配信動作においても、ステップＳ１００からＳ１２８までの処理は、図１０で説明したフローチャートと同様であるので、図示および詳細な説明は繰り返さない。

図１５で説明したように、ステップＳ１２８で得られるライセンスキーＫｃおよび再生回路制御情報ＡＣ２は、秘密鍵Ｋｃｏｍによる暗号化を施されることなくメモリカード１１０固有の公開暗号鍵ＫＰｍ（１）によって暗号化されるので、ステップＳ１３０は省略される。

以下、ステップＳ１２８に続いて、ステップＳ１３２～Ｓ１４２に代えて、ステップＳ１３２ａ～Ｓ１４２ａが実行される。ステップＳ１３２ａ～Ｓ１４２ａのそれぞれにおいては、ステップＳ１３２～Ｓ１４２において取り扱われるライセンスキーＫｃおよび再生回路制御情報ＡＣ２が、暗号化された形｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍから、そのままの形であるＫｃおよびＡＣ２に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図１０で説明したのと同様であるので説明は繰返さない。

図１８には、実施の形態２に従うデータ配信システムにおける再生動作のフローが示される。

図１８を参照して、実施の形態２に従うデータ配信システムにおいて使用される携帯電話機携帯電話機１０１による再生動作においては、図１１に示した実施の形態１に従う再生動作と比較して、ステップＳ２２２～Ｓ２２６に代えて、ステップＳ２２２ａ～Ｓ２２６ａが実行される点で異なる。

ステップＳ２２２ａ～Ｓ２２６ａのそれぞれにおいては、ステップＳ２２２～Ｓ２２６において取り扱われるライセンスキーＫｃおよび再生回路制御情報ＡＣ

２が、暗号化した形｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍから、そのままの形であるＫｃ／／ＡＣ２に代えられて取扱われる点が異なる。その他の暗号化および復号処理については既に図１１で説明したのと同様であるので説明は繰返さない。また、その他のステップについては図１１と同様であるので説明は繰返さない。

図１９および図２０には、実施の形態２に従うデータ配信システムにおける複製動作のフローが示される。

図１９および図２０においては、２つのメモリカード１１０および１１２の間で、実施の形態２に従う携帯電話機１０１および１０３を介してコンテンツデータおよびキーデータ等の複製を行なう処理を説明する。

携帯電話機１０１およびメモリカード１１０についての種類を識別するための自然数をｍ＝１およびｎ＝１とし、携帯電話機１０３およびメモリカード１１２についての種類を識別するため自然数をｍ＝２およびｎ＝２とする。また、メモリカード１１０および１１２を識別するための自然数ｉは、実施の形態１と同様に、それぞれｉ＝１およびｉ＝２であるものとする。

図１９および２０においては、図１２から図１４に示した実施の形態１に従う複製動作のフローチャートと異なる点について説明する。

図１２で説明したステップＳ３００からＳ３３８までの処理は、実施の形態２に従う複製動作においても同様に実行されるので、図示および詳細な説明は繰り返さない。

図１９および図２０を参照して、実施の形態２に従うデータ配信システムにおける複製セッションにおいては、図１３および図１４に示すステップＳ３３４～Ｓ３４４に代えて、ステップＳ３３４ａ～Ｓ３４４ａが実行される点、およびステップＳ２２８が省略される点で異なる。

ステップＳ３３４ａ～Ｓ３４４ａのそれぞれにおいては、ステップＳ３３４～Ｓ３４４において取り扱われるライセンスキーＫｃおよび再生回路制御情報ＡＣ２が、暗号化された形｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍから、そのままの形であるＫｃおよびＡＣ２に代えられて取扱われる点が異なる。また、秘密鍵Ｋｃｏｍによって暗号化されることなく、ライセンスキーＫｃおよび再生制限情報ＡＣ２が与えられるので、ステップＳ２２８は省略される。

その他の暗号化および復号処理については既に図１３および図１４で説明したのと同様であるので説明は繰返さない。

その他のステップについては図１３および図１４と同様であるので説明は繰返さない。

このような構成とすることによって、再生回路に共通な秘密鍵Ｋｃｏｍを用いない構成としても、実施の形態１に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

［実施の形態３］

実施の形態３に従うデータ配信システムにおいては、実施の形態２のデータ配信システムの構成とは異なって、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２がメモリカードにおいて、暗号化されることなく平文にて記録される点を特徴とする。

すなわち、実施の形態３に従う配信システムは、実施の形態２のメモリカード１１０に代えて、メモリカード２１０を備える点で異なる。配信サーバ３１および携帯電話機１０１の構成は同一であるため説明は繰返さない。

図２１を参照して、メモリカード２１０は、メモリカード１１０と比較して、データバスＢＳ４を介してメモリ１４１５とデータの授受が行なわれない点、および、ライセンスキーＫｃと再生回路制御情報ＡＣ２を格納する再生情報制御部１４３０を備える点で異なる。再生情報保持部１４３０は、必ずＴＲＭ領域内に設けられ、データバスＢＳ４との間でデータの授受が可能である。

実施の形態２の場合とは異なり、公開暗号鍵ＫＰｍ（１）にて暗号化された状態でメモリカードに伝達される、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２は、メモリ１４１５に直接格納されない。すなわち、ライセンスキーＫｃおよび再生制御情報ＡＣ２は、復号処理部１４２２によって復号された後、データバスＢＳ４を介して、平文にて再生情報保持部１４３０に保持される。

図２２を参照して、再生情報保持部１４３０は、ライセンス情報保持部１４４０と対応したＮ個のバンクを有し、各ライセンスに対応するライセンスキーＫｃおよび再生回路制御情報ＡＣ２をバンクごとに保持する。このとき、ライセンス情報保持部１４４０に保持された、同一のライセンスに対するライセンスＩＤ、

コンテンツＩＤおよびアクセス制限情報ＡＣ１を保持したバンクと対応したバンクを用いる。

その他の部分の構成については、メモリカード１１０と同様であるため詳細な説明は省略する。なお、メモリカードに対応して定められる自然数ｉ、およびｍは、本来、メモリカード１１０と同一の値になり得ないが、説明を簡略化するために、以下においては、これらの自然数ｉおよびｍは、実施の形態１および２におけるメモリカード１１０と同様に、ｉ＝１およびｍ＝１であるものとして説明する。

実施の形態３に従う配信動作については、フローチャートは図示されていないが、実施の形態２における図１７の配信動作時のフローチャートにおいて、ライセンスの記録を行なうステップＳ１４０ａおよびＳ１４２ａにおける処理を変更すればよい。

ステップＳ１４０ａに相当するステップにおいては、暗号化データ（Ｋｃ／／ＡＣ１／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ２｝Ｋｍ（１）を復号処理部１４２２において秘密復号鍵Ｋｍ（１）を用いて復号し、得られたライセンスキーＫｃおよび再生回路制御情報ＡＣ２を再生情報保持部１４３０に記録する。さらに、ステップＳ１４２ａに相当するステップにおいては、ステップＳ１４０ａに相当するステップにおける復号処理で得られたライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を、ライセンス保持部情報保持部１４４０中の再生情報保持部１４３０と対応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態２の場合と同様であるため説明は繰り返さない。

同様に、実施の形態３に従う再生動作については、フローチャートは図示されていないが、実施の形態２における図１８の再生動作時のフローチャートにおいて、メモリ１４１５からライセンスキーＫｃ、再生回路制御情報ＡＣ２を取得するステップＳ２２２ａにおける処理内容が変更される。すなわち、ステップＳ２２２ａに相当するステップにおいて、再生情報保持部１４３０からライセンスキーＫｃ、再生回路制御情報ＡＣ２を取得する。再生動作の他のステップにおける処理は、実施の形態２の場合と同様であるため説明は繰り返さない。

このように、実施の形態３に従う配信システムは、実施の形態２に従う配信システムに対してメモリカード２１０の内部処理が異なるのみであり、実施の形態２と互換性があり、相互に運用することができる。

同様に、実施の形態３に従う複製動作については、フローチャートが図示されていないが、配信動作および再生動作と同様に、実施の形態２における図１９および図２０の複製動作時のフローチャートにおいて、メモリ１４１５からライセンスキーＫｃ、再生回路制御情報ＡＣ２を取得するステップＳ３３４ａ、ライセンスの記録を行なうステップＳ３４２ａおよびＳ３４４ａにおける処理を変更すればよい。すなわち、ステップＳ３４２ａに相当するステップにおいては、暗号化データ｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）を復号処理部１４２２において秘密復号鍵Ｋｍ（２）を用いて復号し、得られたライセンスキーＫｃおよび再生回路制御情報ＡＣ２を再生情報保持部１４３０に記録する。さらに、ステップＳ３４４ａに相当するステップにおいては、ステップＳ３４２ａに相当するステップにおける復号処理で得られたライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を、ライセンス保持部情報保持部１４４０中の再生情報保持部１４３０と対応するバンクに記録する。

なお、実施の形態２における配信システムにおいては、メモリカード内の動作が異なるのみであるため、実施の形態２のメモリカード１１０と実施の形態３のメモリカード２１０とは相互互換のあるメモリカードであり、その意味において実施の形態２と実施の形態３との配信システムは同一の配信システムで運用することができる。

また、このような実施の形態３に従うメモリカード２１０の適用は、実施の形態１に従う配信システムとの組合せにおいても実行することができる。すなわち、ライセンスキーＫｃおよび再生回路制御情報ＡＣ２を鍵Ｋｃｏｍによって暗号化された｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍの状態で、再生情報保持部１４３０に記録することも可能である。

以下に、このような場合における実施の形態１に従う配信システムにおける処理動作からの変更点を説明する。

実施の形態３を実施の形態１と組合せた場合の配信動作については、実施の形

態１における図１０フローチャートにおいて、ライセンスの記録を行なうステップＳ１４０およびＳ１４２における処理を変更すればよい。

ステップＳ１４０に相当するステップにおいては、暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（１）を復号処理部１４２２において秘密復号鍵Ｋｍ（１）を用いて復号し、得られたライセンスキーＫｃおよび再生回路制御情報ＡＣ２を再生情報保持部１４３０に記録する。さらに、ステップＳ１４２に相当するステップにおいては、ステップＳ１４０に相当するステップにおける復号処理で得られたライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を、ライセンス保持部情報保持部１４４０中の再生情報保持部１４３０と対応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態１の場合と同様であるため説明は繰り返さない。

同様に、実施の形態３を実施の形態１と組合せた場合の再生動作については、実施の形態１における図１１の再生動作時のフローチャートにおいて、メモリ１４１５からライセンスキーＫｃ、再生回路制御情報ＡＣ２を取得するステップＳ２２２における処理内容が変更される。すなわち、ステップＳ２２２に相当するステップにおいて、ライセンスキーＫｃ、再生回路制御情報ＡＣ２を｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍの形で再生情報保持部１４３０から取得する。再生動作の他のステップにおける処理は、実施の形態１の場合と同様であるため説明は繰り返さない。

同様に、実施の形態３を実施の形態１と組合せた場合の複製動作については、配信動作および再生動作と同様に、実施の形態１における図１３および図１４の複製動作時のフローチャートにおいて、メモリ１４１５からライセンスキーＫｃおよび再生回路制御情報ＡＣ２を｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍの形で取得するステップＳ３３４、ライセンスの記録を行なうステップＳ３４２およびＳ３４４における処理を変更すればよい。すなわち、ステップＳ３４２に相当するステップにおいては、暗号化データ｛｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ（２）を復号処理部１４２２において秘密復号鍵Ｋｍ（２）を用いて復号し、得られた｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍを再生情

報保持部１４３０に記録する。さらに、ステップＳ３４４に相当するステップにおいては、ステップＳ３４２に相当するステップにおける復号処理で得られたライセンスＩＤ、コンテンツＩＤおよびアクセス制限情報ＡＣ１を、ライセンス保持部情報保持部１４４０中の再生情報保持部１４３０と対応するバンクに記録する。

このように、実施の形態３に従う配信システムは、実施の形態１に従う配信システムに対してメモリカード２１０の内部処理が異なるのみであり、実施の形態１と互換性があり、相互に運用することができる。

なお、実施の形態１における配信システムにおいては、メモリカード内の動作が異なるのみであるため、実施の形態１のメモリカード１１０と実施の形態３のメモリカード２１０とは相互互換のあるメモリカードであり、その意味において実施の形態１と実施の形態３とを組合せて同一の配信システムで運用することができる。

なお、図２１においては、ＴＲＭ領域に配置される再生情報保持部１４３０およびライセンス保持部情報保持部１４４０を独立した機能を有するブロックとして示したが、両者を共通のメモリとして配置することも可能である。また、実施の形態１で述べたように、メモリ１４１５をＴＲＭ領域に配置することも可能であるが、この場合において、メモリ１４１５、再生情報保持部１４３０およびライセンス保持部情報保持部１４４０を共通の同一メモリ上に設けることも可能である。

なお、以上で説明したすべての実施の形態においては、複製動作時において、一度に複数のライセンスが複製できる構成について説明したが、一度の複製動作では、１つのライセンスが複製可能なように構成することも可能である。この場合においては、実施の形態１における図１３ならびに、実施の形態２および３における図２０に示したフローチャートからステップＳ３２４を省略して、ステップＳ３２６において、複製ライセンス数が“１”であるとして判断する処理とすればよい。

また、ライセンスの複製は、アクセス制限情報ＡＣ１の所有ライセンス数Ｓｕｂ＿ｍｏｖｅの制約上必ず制限を受けるように説明したが、コンテンツデータの

著作権を所有する著作権者が自由に複製することを許可した場合には、自由な複製が可能となる。この場合には、たとえば所有ライセンス数Ｓｕｂ＿ｍｏｖｅに新たな値、たとえばＦＥ（ｈ）を追加して、Ｓｕｂ＿ｍｏｖｅ＝ＦＥ（ｈ）であれば複製自由とし、図１３に示したフローチャート中のステップＳ３２２の判断処理において、Ｓｕｂ＿ｍｏｖｅ＝ＦＥ（ｈ）の場合に新しい分岐を設けて、ライセンス処理部からＡＣ１を取得する処理を得た後、Ｓｕｂ＿ｍｏｖｅ＝ＦＥ（ｈ）であればステップＳ３３２に移行する処理を行なうことで実現することができる。

また、以上で説明したすべての実施の形態においては、配信動作において、携帯電話機１００から２つの認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａおよび｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａを送信して配信サーバ１０において２つの認証データに対して認証処理をする構成について説明した。

しかし、メモリカード１１０は着脱可能であることから、音楽を再生する場合にコンテンツ再生回路が必ずしも配信を受けた携帯電話機１００である必然性がない。さらに、メモリカード１００が再生動作において再生するコンテンツ再生回路の認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａによって認証処理を行なっているので、配信サーバ１０においてコンテンツ再生回路の認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａによってコンテンツ再生回路（携帯電話機１００）の認証処理を行なわなくてもセキュリティの低下にはつながらない。

したがって、配信サーバ１０に対して、メモリカード１００の認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａのみを送信し、配信サーバ１０においては、配信先のメモリカード１１０の認証データ｛ＫＰｍｃ（１）／／Ｃｍｃ（１）｝ＫＰｍａのみを中心にして復号し認証処理を行なう構成としても同様の効果を得ることができる。

この場合には、すべての実施の形態が参照する図９に示されたフローチャートにおいて、ステップＳ１０４、Ｓ１０６、Ｓ１０８、Ｓ１１０の各処理において、携帯電話機（コンテンツ再生回路）１００の認証データ｛ＫＰｐ（１）／／Ｃｐ（１）｝ＫＰｍａ、公開暗号鍵ＫＰｐ（１）およびクラス証明書Ｃｐ（１）に対する処理を省略することによって、コンテンツ再生回路に対する認証を省略し

た認証処理を行なうことができる。

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

産業上の利用可能性

この発明によるデータ配信システムおよび記録装置は、携帯電話機のような移動通信端末を利用したデータ配信に用いることができる。

【図面の簡単な説明】

図１は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図２は、実施の形態１に従うデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

図３は、実施の形態１に従うデータ配信システムにおいて使用される鍵データ等の特性をまとめて説明する図である。

図４は、図１に示されたライセンスサーバの構成を示す概略ブロック図である。

図５は、図１に示された携帯電話機の構成を示す概略ブロック図である。

図６は、図５に示されたメモリカードの構成を示す概略ブロック図である。

図７は、ライセンス情報保持部に格納される情報の構成を説明する概念図である。

図８は、アクセス制限情報ＡＣ１の内容を説明する図である。

図９は、実施の形態１に従うデータ配信システムにおける配信セッション時の動作を説明するための第１のフローチャートである。

図１０は、実施の形態１に従うデータ配信システムにおける配信セッション時の動作を説明するための第２のフローチャートである。

図１１は、実施の形態１に従う再生セッション時の動作を説明するためのフローチャートである。

図１２は、実施の形態１に従う２つのメモリカード間の複製セッション時の動

作を説明するための第１のフローチャートである。

図１３は、実施の形態１に従う２つのメモリカード間の複製セッション時の動作を説明するための第２のフローチャートである。

図１４は、実施の形態１に従う２つのメモリカード間の複製セッション時の動作を説明するための第３のフローチャートである。

図１５は、実施の形態２に従うライセンスサーバの構成を示す概略ブロック図である。

図１６は、実施の形態２に従う携帯電話機の構成を示す概略ブロック図である。

図１７は、実施の形態２に従うデータ配信システムにおける配信動作を説明するためのフローチャートである。

図１８は、実施の形態２に従う再生動作を説明するフローチャートである。

図１９は、実施の形態２に従うデータ配信システムにおける２つのメモリカード間の複製セッション時の動作を説明するための第１のフローチャートである。

図２０は、実施の形態２に従うデータ配信システムにおける２つのメモリカード間における複製セッション時の動作を説明する第２のフローチャートである。

図２１は、実施の形態３に従うメモリカードの構成を示す概略ブロック図である。

図２２は、再生情報保持部およびライセンス情報保持部に格納される情報の構成を説明する概念図である。

【図１】

*FIG.1*

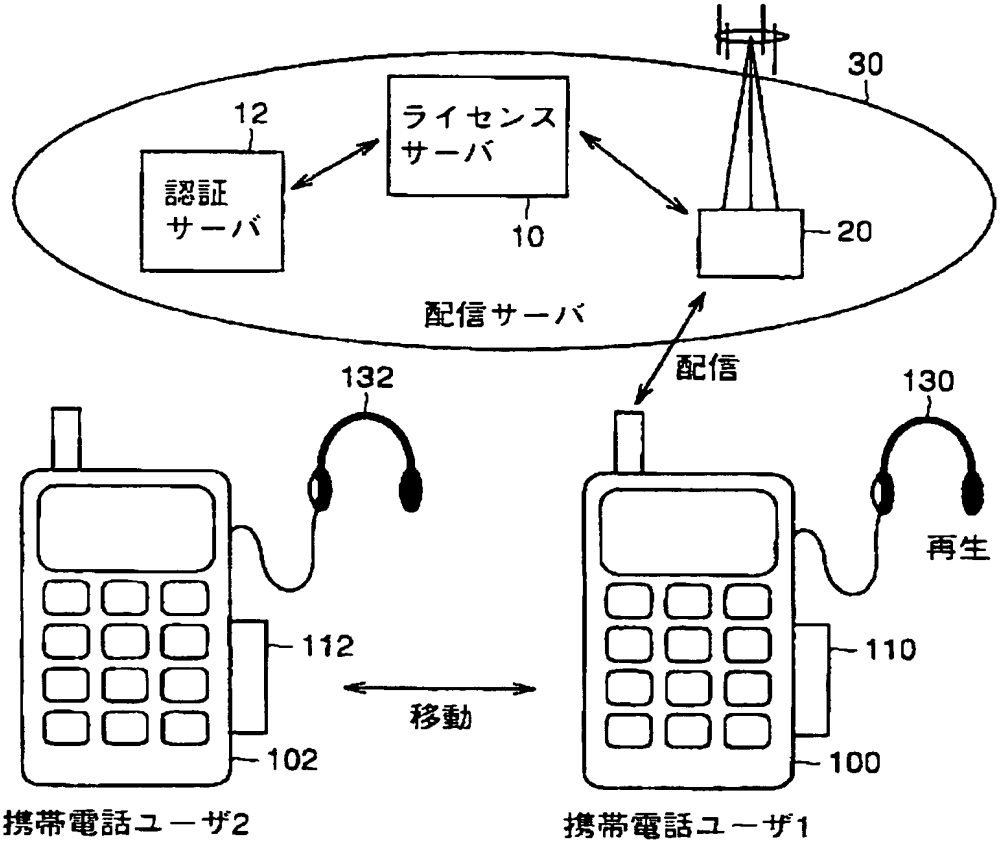

30
12
ライセンス
サーバ
認証
サーバ
10
20
配信サーバ
配信
132
130
再生
112
110
移動
102
100
携帯電話ユーザ2
携帯電話ユーザ1

FIG.2

| 名称 | 属性 | 保持／発生箇所 | 機能・特徴 |
|---|---|---|---|
| Data | コンテンツデータ | 配信サーバ | 例：音楽データ |
| Kc | ライセンスキー | | 暗号化コンテンツデータの復号鍵 |
| {Data}Kc | 暗号化コンテンツデータ | | 共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。 |
| Data-inf | 付加情報 | | 例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報 |
| コンテンツID | コンテンツに関する情報 | | コンテンツデータDataを識別するコード |
| ライセンスID | ライセンスに関する情報 | | ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可） |
| AC | ライセンス購入条件 | | 利用者側から指定(例：ライセンス数,機能限定等) |
| AC1 | アクセス制限情報 | | メモリのアクセスに対する制限(例：再生可能回数) |
| AC2 | 再生回路制御情報 | | コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否） |



WO2001/43342

FIG.3

| 名称 | 属性 | 保持／発生箇所 | 機能・特徴 |
|---|---|---|---|
| KPp(n) | 公開暗号化鍵<br>（非対称鍵） | 携帯電話機 | Kp(n)にて復号可能。<br>{KPp(n)//Cp(n)}KPmaの形式で出荷時に記録<br>nは携帯電話機の種類を区別する値。 |
| KPmc(m) | 公開暗号化鍵<br>（非対称鍵） | メモリカード | Kmcにて復号可能。<br>{KPmc(m)//Cmc(m)}KPmaの形式で出荷時に記録<br>mはメモリカードの種類を区別する値。 |
| Kp(n) | 秘密復号鍵 | 携帯電話機 | コンテンツ再生回路（携帯電話機）固有の復号鍵<br>nは携帯電話機の種類を区別する値。 |
| Kmc(m) | 秘密復号鍵 | メモリカード | メモリカード固有の復号鍵<br>mはメモリカードの種類を区別する値。 |
| Cp(n) | クラス証明書 | 携帯電話機 | コンテンツ再生回路のクラス証明書。<br>{KPp(n)//Cp(n)}KPmaの形式で出荷時に記録<br>nは携帯電話機の種類を区別する値。 |
| Cmc(m) | | メモリカード | メモリカードのクラス証明書。<br>{KPmc(m)//Cmc(m)}KPmaの形式で出荷時に記録<br>mはメモリカードの種類を区別する値。 |
| Ks1 | 共通鍵<br>（セッション固有） | 配信サーバ | 配信セッション毎に発生 |
| Ks2 | | メモリカード | 配信／移動(受)セッション毎に発生 |
| Ks3 | | メモリカード | 再生／移動(送)セッション毎に発生 |
| Ks4 | | 携帯電話機 | 再生セッション毎に発生 |
| Km(i) | 秘密復号鍵 | メモリカード | メモリカードごと(i)に固有の復号鍵<br>KPm(I)で暗号化されたデータはKm(i)で復号可能 |
| KPm(i) | 公開暗号化鍵<br>（非対称鍵） | メモリカード | メモリカードごと(i)に固有の暗号化鍵 |
| KPma | 認証鍵<br>（公開復号鍵） | 配信サーバ | 配信システム全体で共通。 |
| Kcom | 秘密復号鍵 | 携帯電話機<br>配信サーバ | 再生回路共通の秘密鍵。Kc,AC2の暗号化および復号に利用。<br>（共通鍵方式,公開鍵方式のいずれであっても可） |

【図３】



WO2001/43342

【図４】

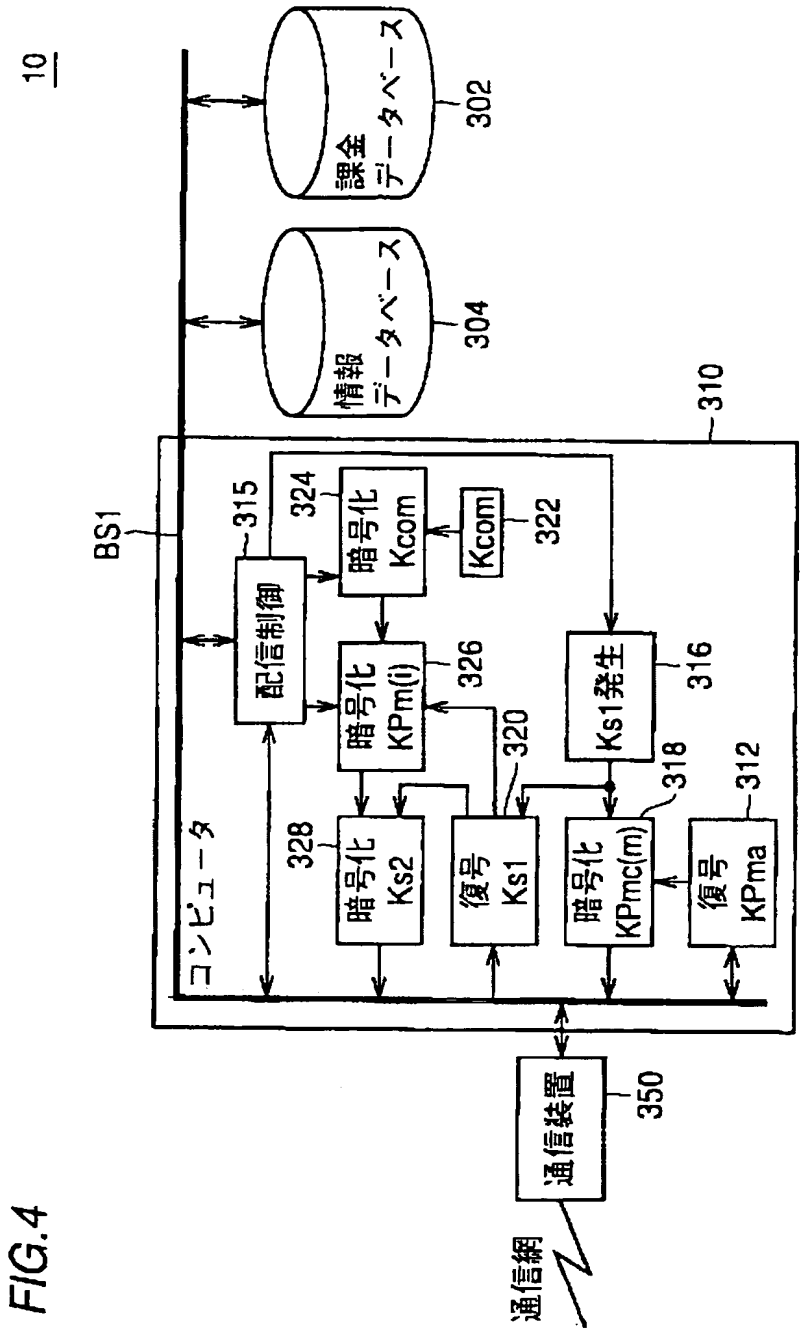

10
課金データベース
302
情報データベース
304
310
BS1
315
324
暗号化 Kcom
Kcom
322
配信制御
暗号化 KPm(i)
326
Ks1発生
316
320
318
312
328
暗号化 Ks2
復号 Ks1
暗号化 KPmc(m)
復号 KPma
コンピュータ
通信装置
350
通信網

FIG.4

【図５】

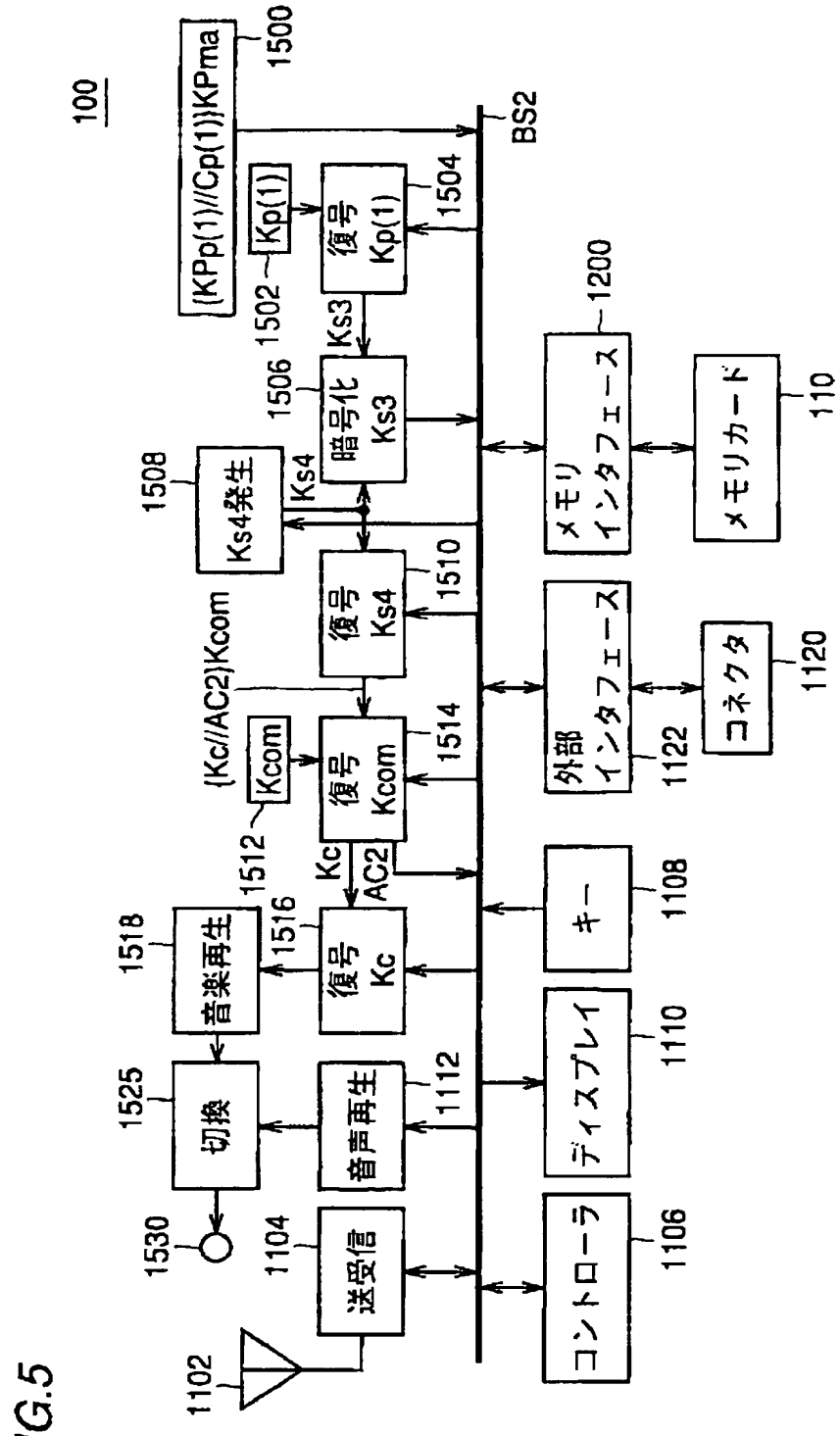

100
{KPp(1)//Cp(1)}KPma
1500
BS2
Kp(1)
1502
復号 Kp(1)
1504
Ks3
1506
暗号化 Ks3
1200
メモリ インタフェース
メモリカード
110
1508
Ks4発生
Ks4
{Kc//AC2}Kcom
Kcom
復号 Ks4
1510
外部 インタフェース
コネクタ
1120
1122
復号 Kcom
1514
Kc
AC2
1512
1518
音楽再生
1516
復号 Kc
キー
1108
1525
切換
音声再生
1112
ディスプレイ
1110
1530
1104
送受信
コントローラ
1106
1102

FIG.5

【図６】

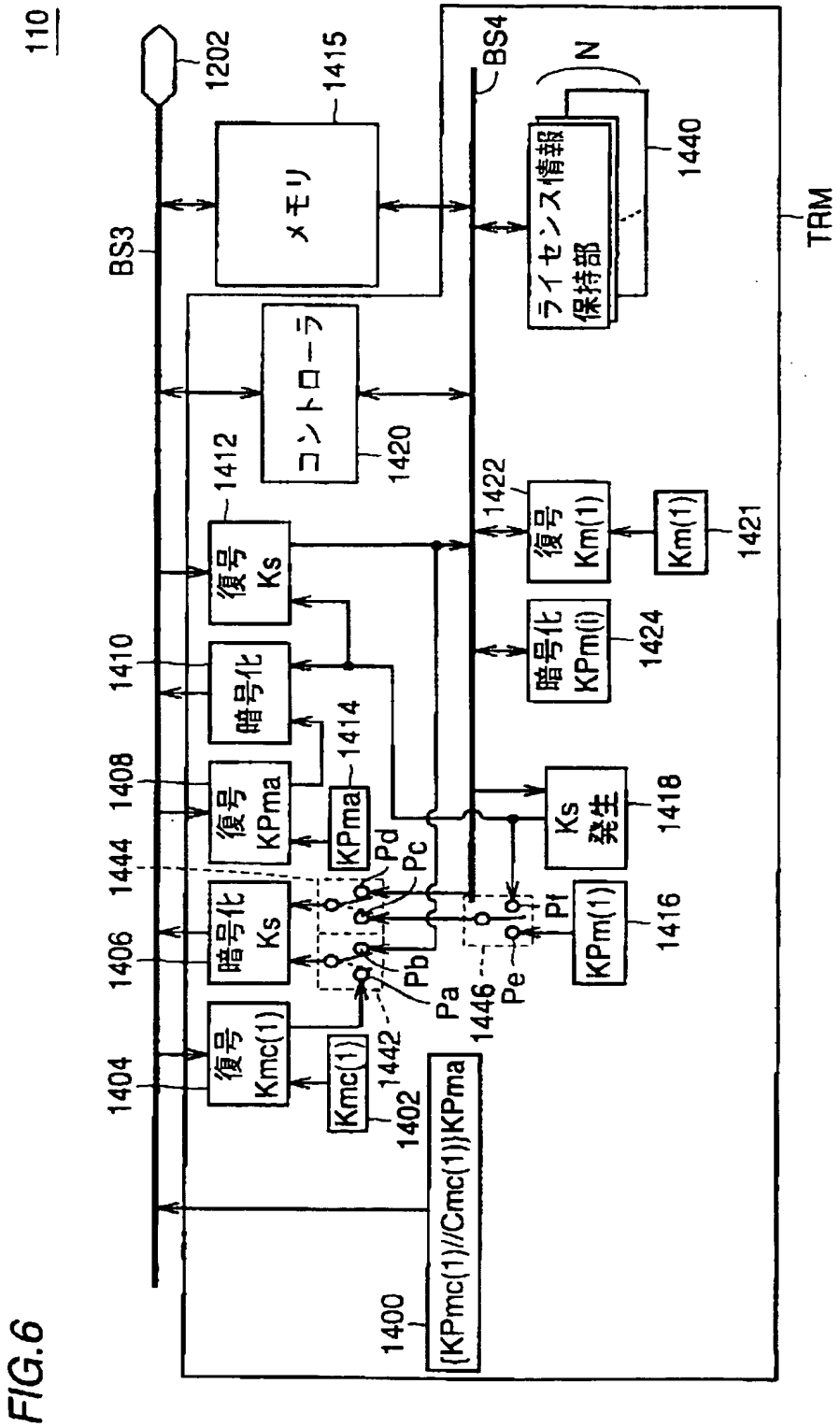
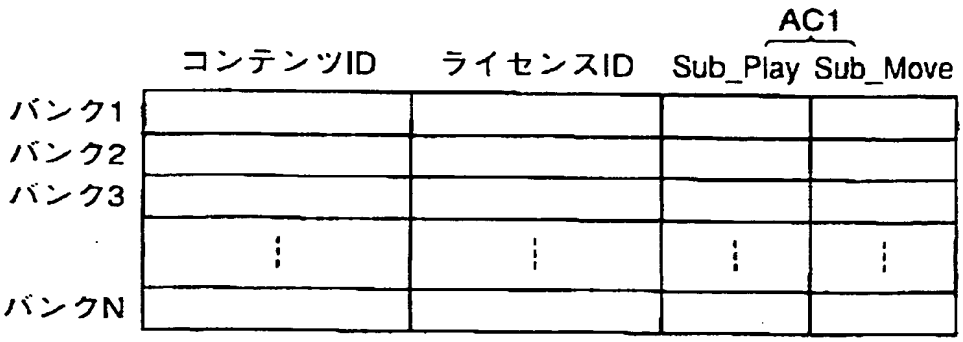

110
1202
1415
BS4
N
BS3
メモリ
ライセンス情報
保持部
1440
TRM
コントローラ
1420
1412
1422
復号
Ks
復号
Km(1)
Km(1)
1421
1410
暗号化
暗号化
KPm(i)
1424
1414
1408
復号
KPma
KPma
Pd
Pc
Ks
発生
1418
1444
暗号化
Ks
Pf
1406
Pb
Pa
1446
Pe
KPm(1)
1416
1404
復号
Kmc(1)
Kmc(1)
1442
1402
{KPmc(1)//Cmc(1)}KPma
1400

FIG.6

【図７】

FIG.7



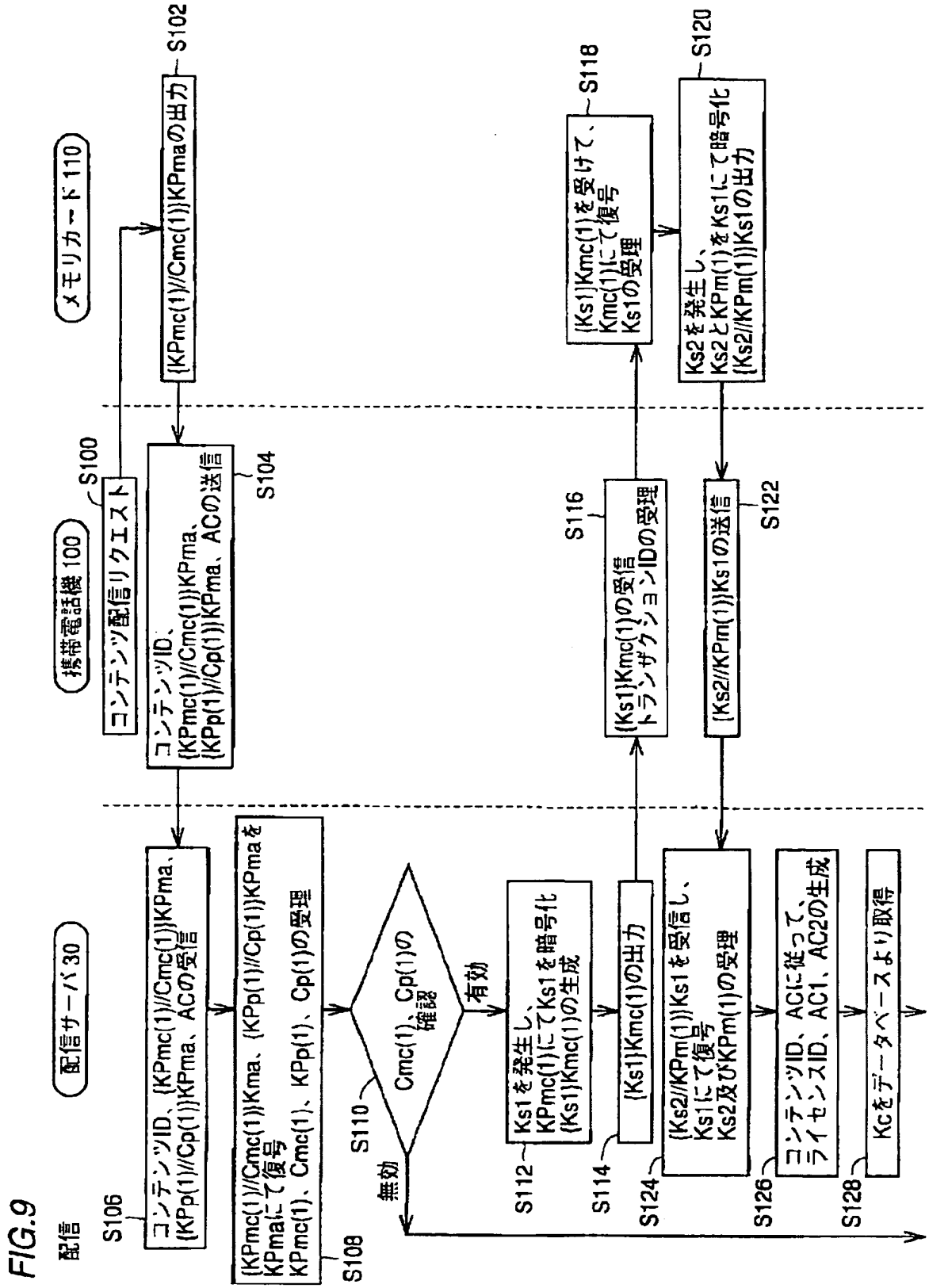

【図８】

FIG.8

| AC1 | Sub_Play | 再生回数制限 |
|---|---|---|
| | | 0 ：再生不能 |
| | | 1～7F(h) ：再生可能回数 |
| | | 80～FE(h)：未使用 |
| | | FF(h) ：制限なし |
| | Sub_Move | 所有ライセンス数 |
| | | 0 ：ライセンス無 |
| | | 1～7F(h) ：所有ライセンス数 |
| | | 80～FE(h) ：未使用 |
| | | FF(h) ：移動禁止 |

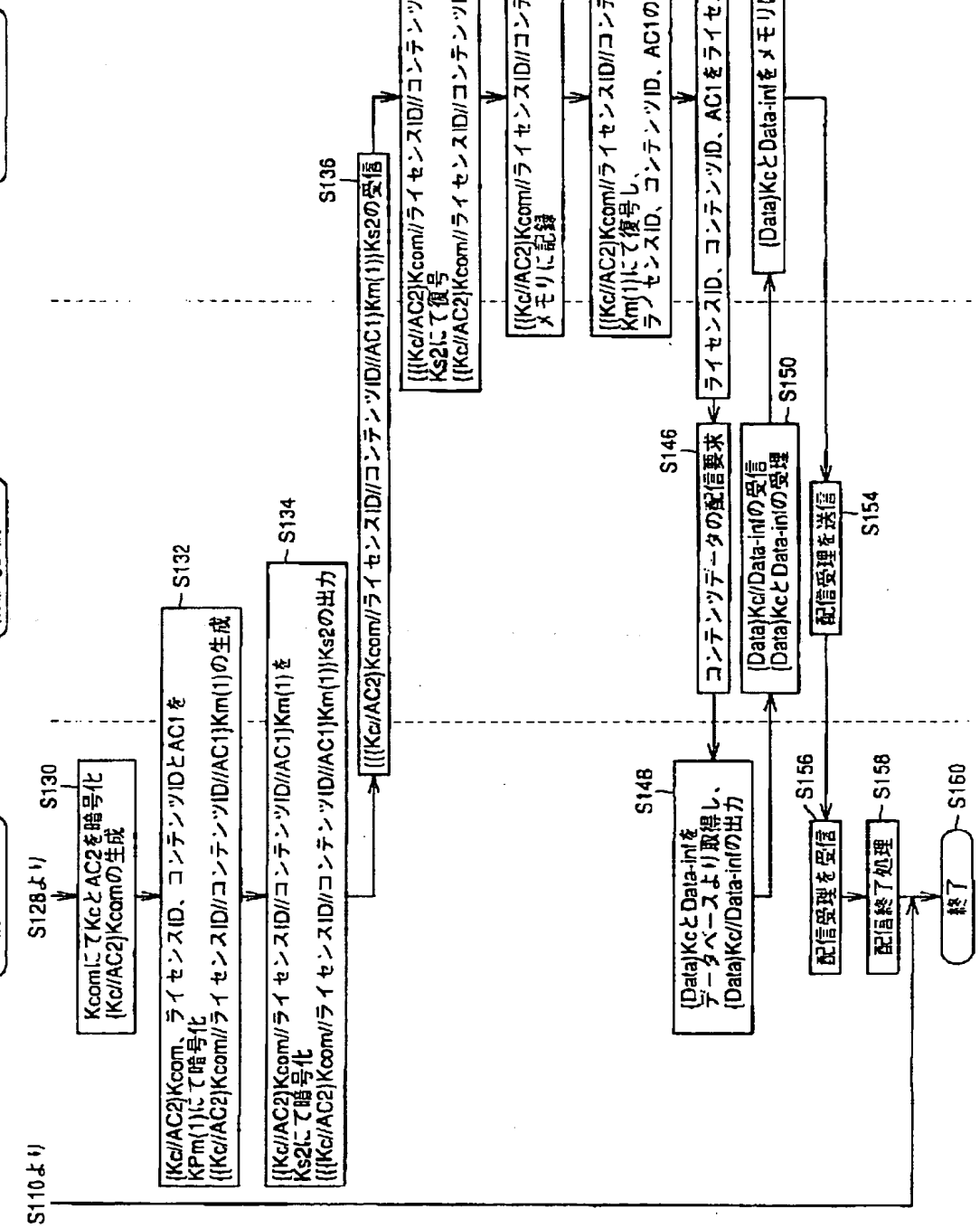
【図９】

FIG.9


配信
配信サーバ30
携帯電話機100
メモリカード110
コンテンツID、{KPmc(1)//Cmc(1)}KPma、{KPp(1)//Cp(1)}KPma、ACの受信
S106
{KPmc(1)//Cmc(1)}Kma、{KPp(1)//Cp(1)}KPmaを KPmaにて復号 KPmc(1)、Cmc(1)、KPp(1)、Cp(1)の受理
S108
Cmc(1)、Cp(1)の確認
S110
無効
有効
Ks1を発生し、KPmc(1)にてKs1を暗号化{Ks1}Kmc(1)の生成
S112
{Ks1}Kmc(1)の出力
S114
{Ks1}Kmc(1)の受信 トランザクションIDの受理
S116
{Ks1}Kmc(1)を受けて、Kmc(1)にて復号 Ks1の受理
S118
{Ks2//KPm(1)}Ks1を受信し、Ks1にて復号 Ks2及びKPm(1)の受理
S124
Ks2を発生し、Ks2とKPm(1)をKs1にて暗号化{Ks2//KPm(1)}Ks1の出力
S120
{Ks2//KPm(1)}Ks1の送信
S122
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S126
Kcをデータベースより取得
S128
S130へ
S160へ
コンテンツ配信リクエスト
S100
{KPmc(1)//Cmc(1)}KPmaの出力
S102
コンテンツID、{KPmc(1)//Cmc(1)}KPma、{KPp(1)//Cp(1)}KPma、ACの送信
S104

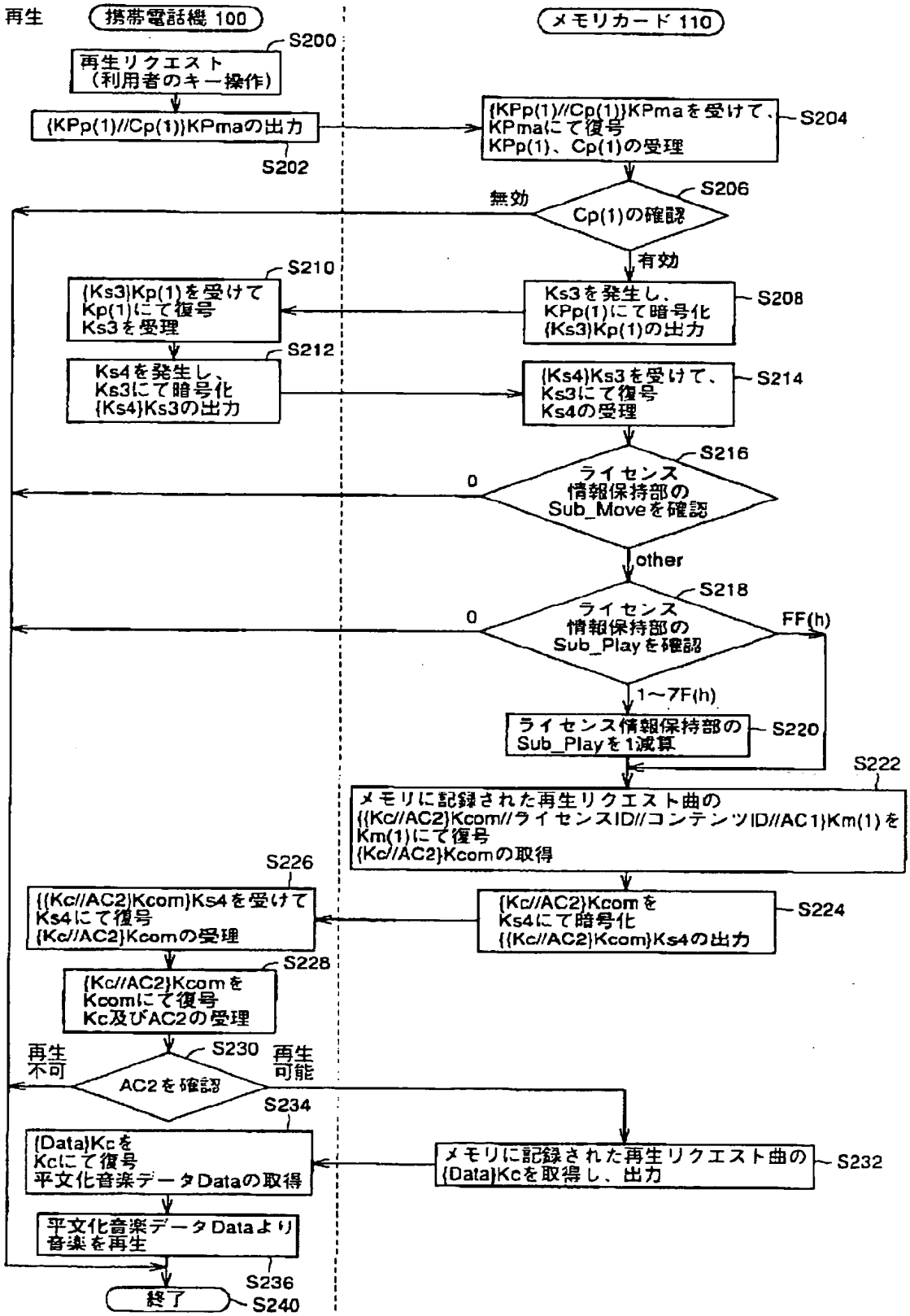
【図１０】

FIG.10


配信サーバ30
携帯電話機100
メモリカード110
S110より
S128より
S130
KcomにてKcとAC2を暗号化
{Kc//AC2}Kcomの生成
S132
{Kc//AC2}Kcom、ライセンスID、コンテンツIDとAC1を
KPm(1)にて暗号化
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)の生成
S134
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
Ks2にて暗号化
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)}Ks2の出力
S136
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)}Ks2の受信
S138
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)}Ks2を
Ks2にて復号
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)の受理
S140
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
メモリに記録
S142
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S144
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S146
コンテンツデータの配信要求
S148
{Data}KcとData-inlを
データベースより取得し、
{Data}Kc//Data-inlの出力
S150
{Data}Kc//Data-inlの受信
{Data}KcとData-inlの受理
S152
{Data}KcとData-inlをメモリに記録
S154
配信受理を送信
S156
配信受理を受信
S158
配信終了処理
S160
終了

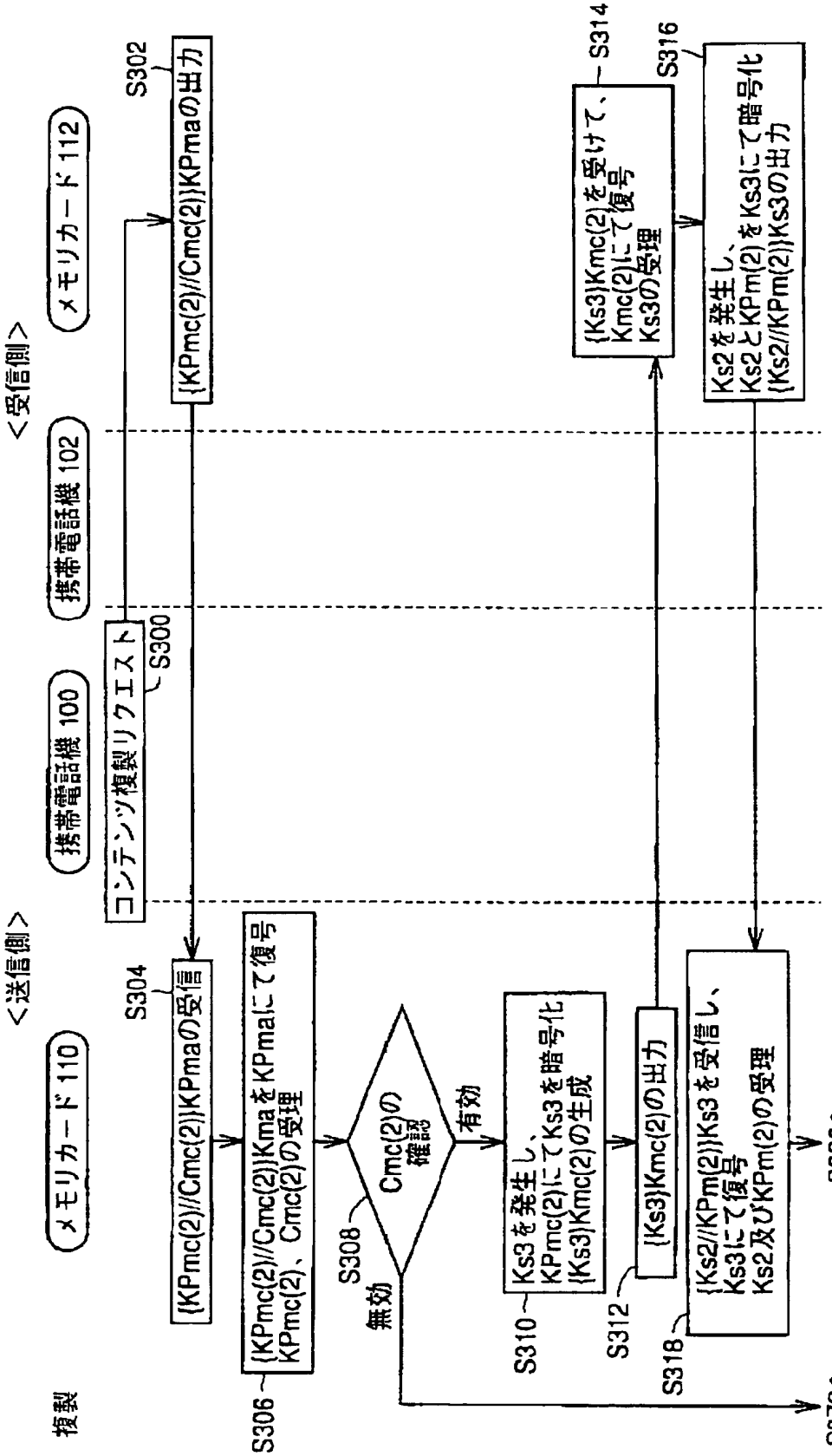
【図１１】

FIG.11


再生
携帯電話機 100
メモリカード 110
S200
再生リクエスト
(利用者のキー操作)
{KPp(1)//Cp(1)}KPmaの出力
S202
{KPp(1)//Cp(1)}KPmaを受けて、
KPmaにて復号
KPp(1)、Cp(1)の受理
S204
S206
Cp(1)の確認
無効
有効
S208
Ks3を発生し、
KPp(1)にて暗号化
{Ks3}Kp(1)の出力
S210
{Ks3}Kp(1)を受けて
Kp(1)にて復号
Ks3を受理
S212
Ks4を発生し、
Ks3にて暗号化
{Ks4}Ks3の出力
S214
{Ks4}Ks3を受けて、
Ks3にて復号
Ks4の受理
S216
ライセンス
情報保持部の
Sub_Moveを確認
0
other
S218
ライセンス
情報保持部の
Sub_Playを確認
0
FF(h)
1～7F(h)
S220
ライセンス情報保持部の
Sub_Playを1減算
S222
メモリに記録された再生リクエスト曲の
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号
{Kc//AC2}Kcomの取得
S224
{Kc//AC2}Kcomを
Ks4にて暗号化
{{Kc//AC2}Kcom}Ks4の出力
S226
{{Kc//AC2}Kcom}Ks4を受けて
Ks4にて復号
{Kc//AC2}Kcomの受理
S228
{Kc//AC2}Kcomを
Kcomにて復号
Kc及びAC2の受理
S230
AC2を確認
再生
不可
再生
可能
S232
メモリに記録された再生リクエスト曲の
{Data}Kcを取得し、出力
S234
{Data}Kcを
Kcにて復号
平文化音楽データDataの取得
平文化音楽データDataより
音楽を再生
S236
終了
S240

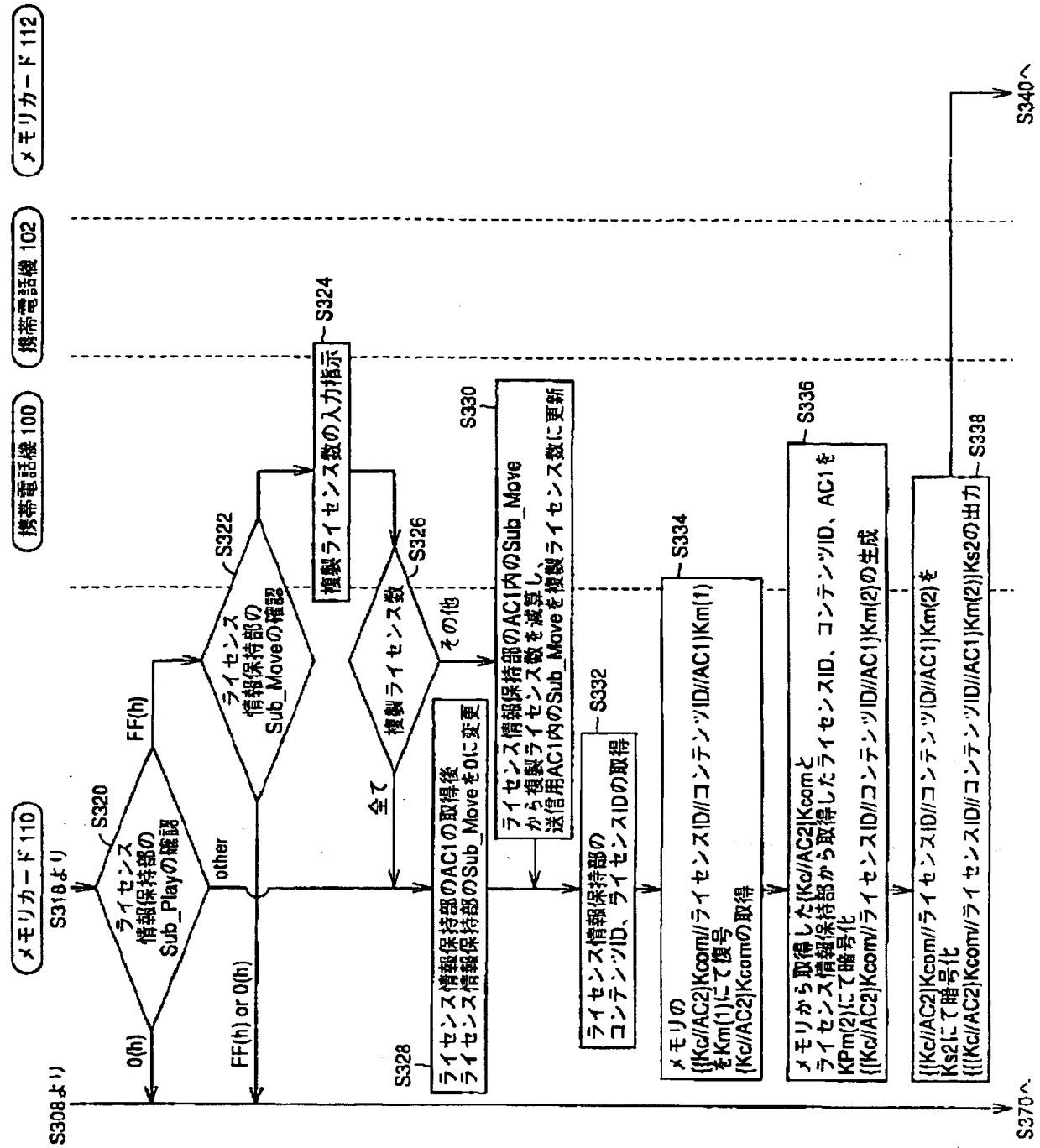
【図１２】

FIG.12


複製
<送信側>
メモリカード 110
携帯電話機 100
<受信側>
携帯電話機 102
メモリカード 112
コンテンツ複製リクエスト
S300
S302
{KPmc(2)//Cmc(2)}KPmaの出力
S304
{KPmc(2)//Cmc(2)}KPmaの受信
S306
{KPmc(2)//Cmc(2)}KmaをKPmaにて復号
KPmc(2)、Cmc(2)の受理
S308
Cmc(2)の確認
有効
無効
S310
Ks3を発生し、
KPmc(2)にてKs3を暗号化
{Ks3}Kmc(2)の生成
S312
{Ks3}Kmc(2)の出力
S314
{Ks3}Kmc(2)を受けて、
Kmc(2)にて復号
Ks3の受理
S316
Ks2を発生し、
Ks2とKPm(2)をKs3にて暗号化
{Ks2//KPm(2)}Ks3の出力
S318
{Ks2//KPm(2)}Ks3を受信し、
Ks3にて復号
Ks2及びKPm(2)の受理
S320へ
S370へ

【図１３】

FIG.13


メモリカード110
携帯電話機100
携帯電話機102
メモリカード112
S308より
S318より
S320
ライセンス情報保持部のSub_Playの確認
0(h)
FF(h)
other
FF(h) or 0(h)
S322
ライセンス情報保持部のSub_Moveの確認
S324
複製ライセンス数の入力指示
全て
S326
複製ライセンス数
その他
S328
ライセンス情報保持部のAC1の取得後ライセンス情報保持部のSub_Moveを0に変更
S330
ライセンス情報保持部のAC1内のSub_Moveから複製ライセンス数を減算し、送信用AC1内のSub_Moveを複製ライセンス数に更新
S332
ライセンス情報保持部のコンテンツID、ライセンスIDの取得
S334
メモリの{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(1)をKm(1)にて復号{Kc//AC2}Kcomの取得
S336
メモリから取得した{Kc//AC2}Kcomとライセンス情報保持部から取得したライセンスID、コンテンツID、AC1をKPm(2)にて暗号化{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の生成
S338
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)をKs2にて暗号化{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2の出力
S340へ
S370へ

【図１４】

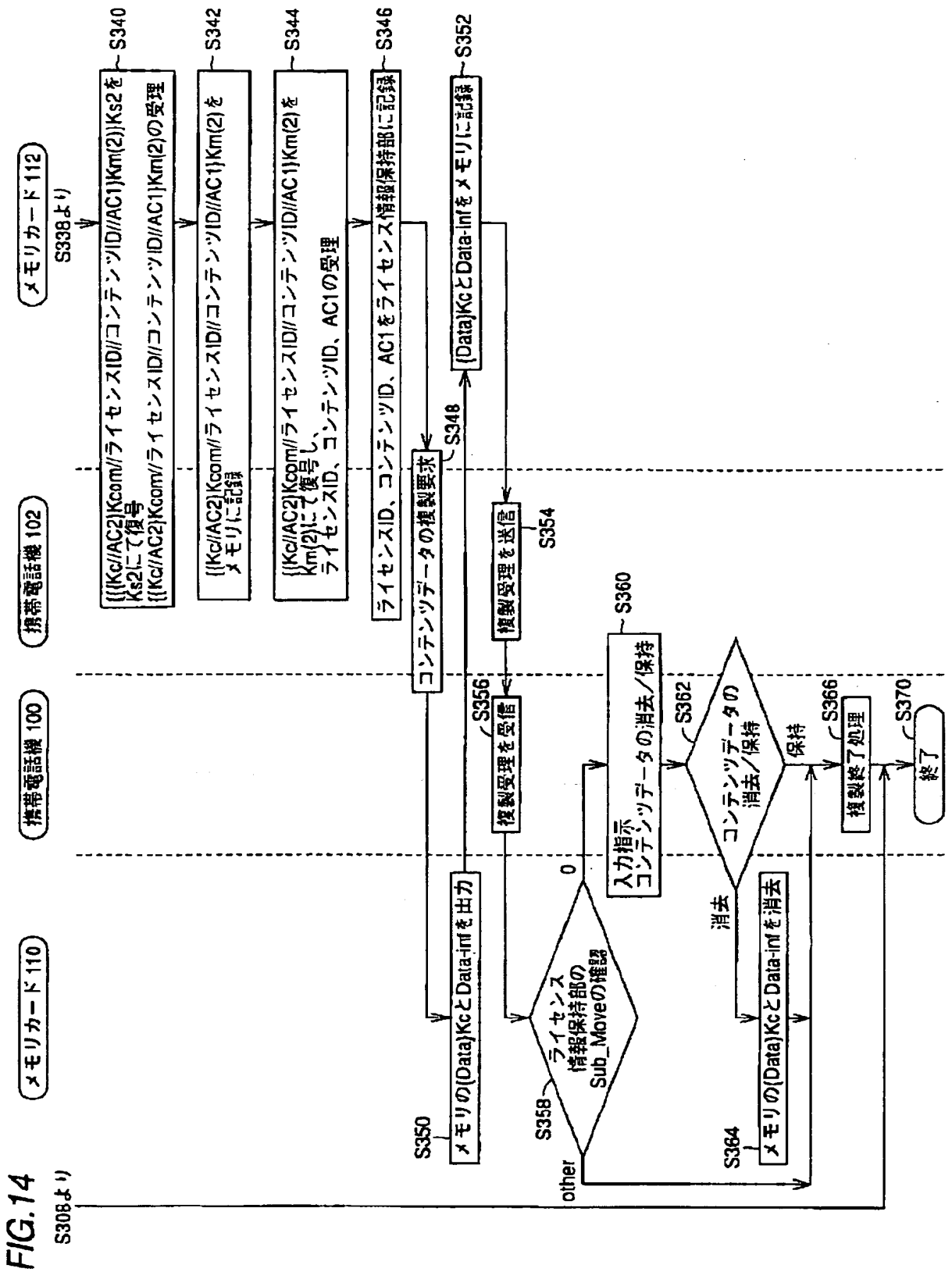

メモリカード110
携帯電話機100
携帯電話機102
メモリカード112
S308より
S338より
S340
{{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)}Ks2を
Ks2にて復号
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)の受理
S342
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
メモリに記録
S344
{{Kc//AC2}Kcom//ライセンスID//コンテンツID//AC1}Km(2)を
Km(2)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S346
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S348
コンテンツデータの複製要求
S352
{Data}KcとData-infをメモリに記録
S354
複製受理を送信
S356
複製受理を受信
S358
ライセンス
情報保持部の
Sub_Moveの権限
0
other
S360
入力指示
コンテンツデータの消去／保持
S362
コンテンツデータの
消去／保持
消去
保持
S364
メモリの{Data}KcとData-infを消去
S366
複製終了処理
S370
終了
S350
メモリの{Data}KcとData-infを出力

FIG.14

【図１５】

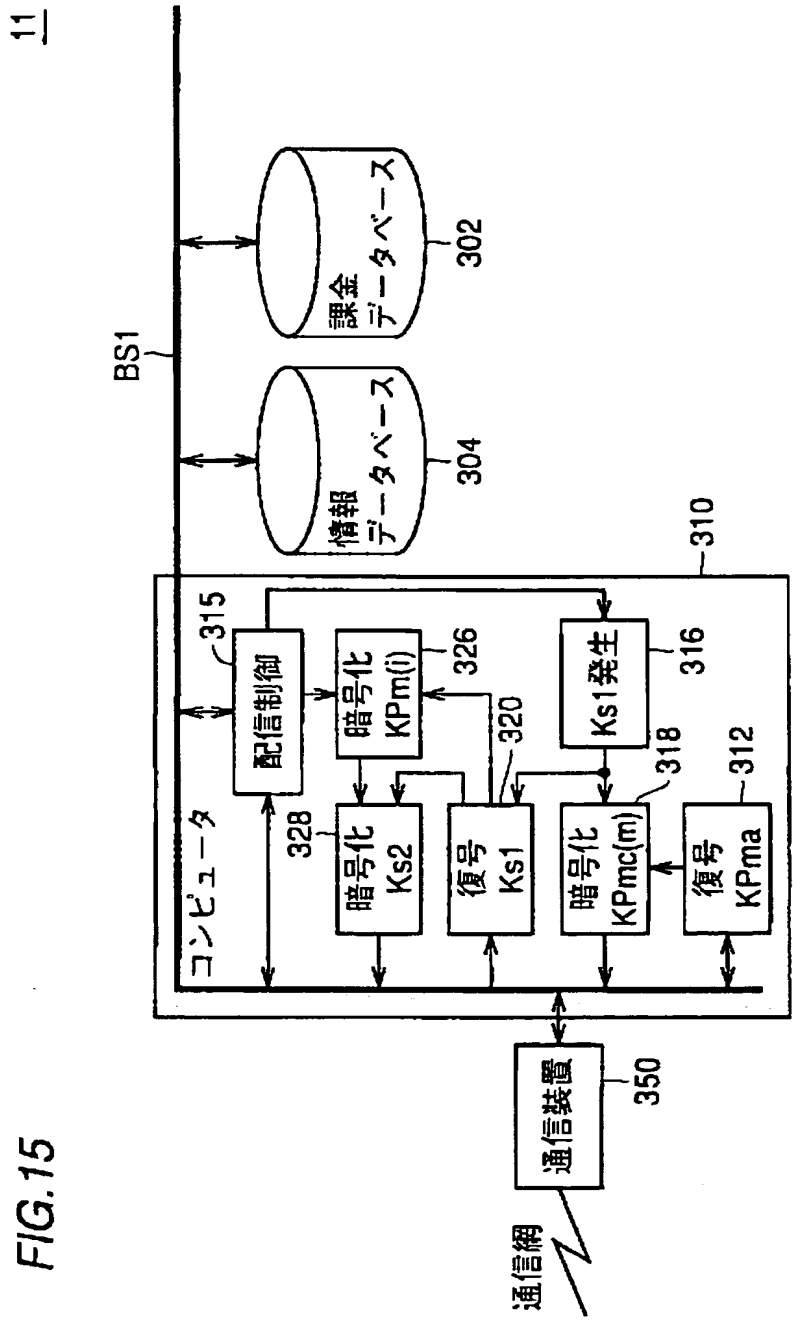

11
BS1
課金データベース
302
情報データベース
304
310
315
配信制御
326
暗号化 KPm(i)
316
Ks1発生
320
318
312
328
暗号化 Ks2
復号 Ks1
暗号化 KPmc(m)
復号 KPma
コンピュータ
通信装置
350
通信網

FIG.15

【図１６】

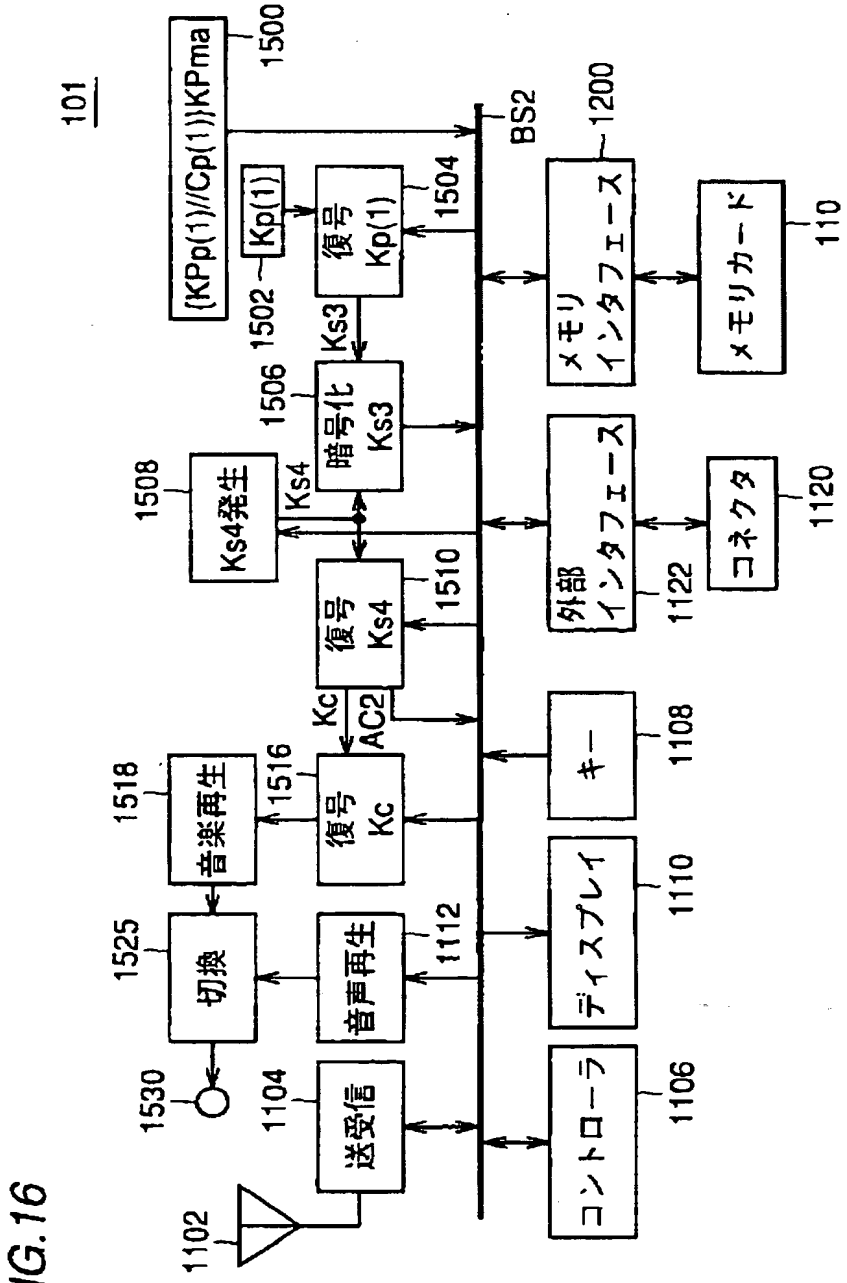
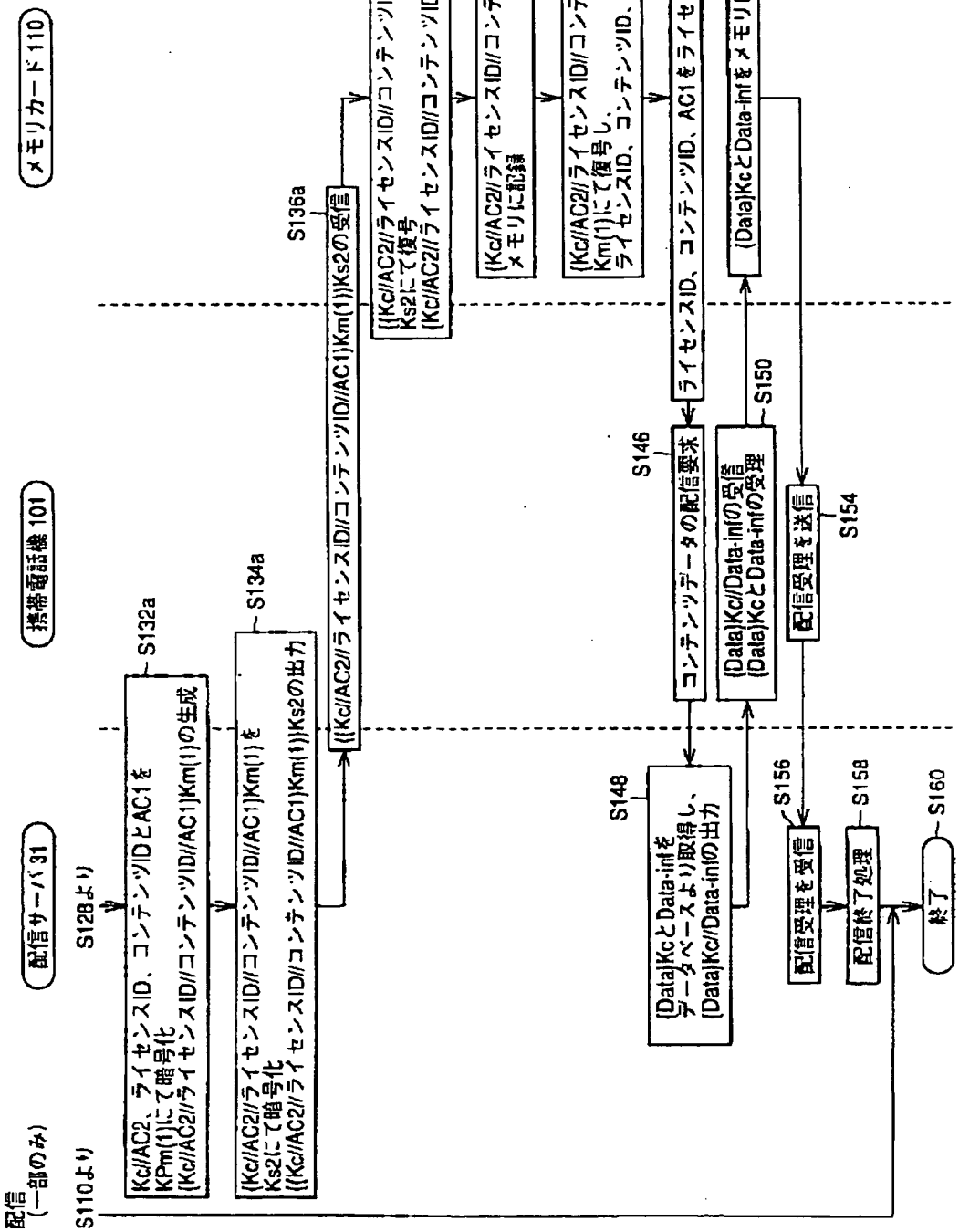

101
[KPp(1)//Cp(1)]KPma
1500
BS2
1200
メモリ
インタフェース
メモリカード
110
Kp(1)
1502
復号
Kp(1)
1504
Ks3
1506
暗号化
Ks3
1508
Ks4発生
Ks4
復号
Ks4
1510
外部
インタフェース
1122
コネクタ
1120
Kc
AC2
1518
音楽再生
1516
復号
Kc
キー
1108
1525
切換
1112
音声再生
ディスプレイ
1110
1530
1104
送受信
コントローラ
1106
1102

FIG.16

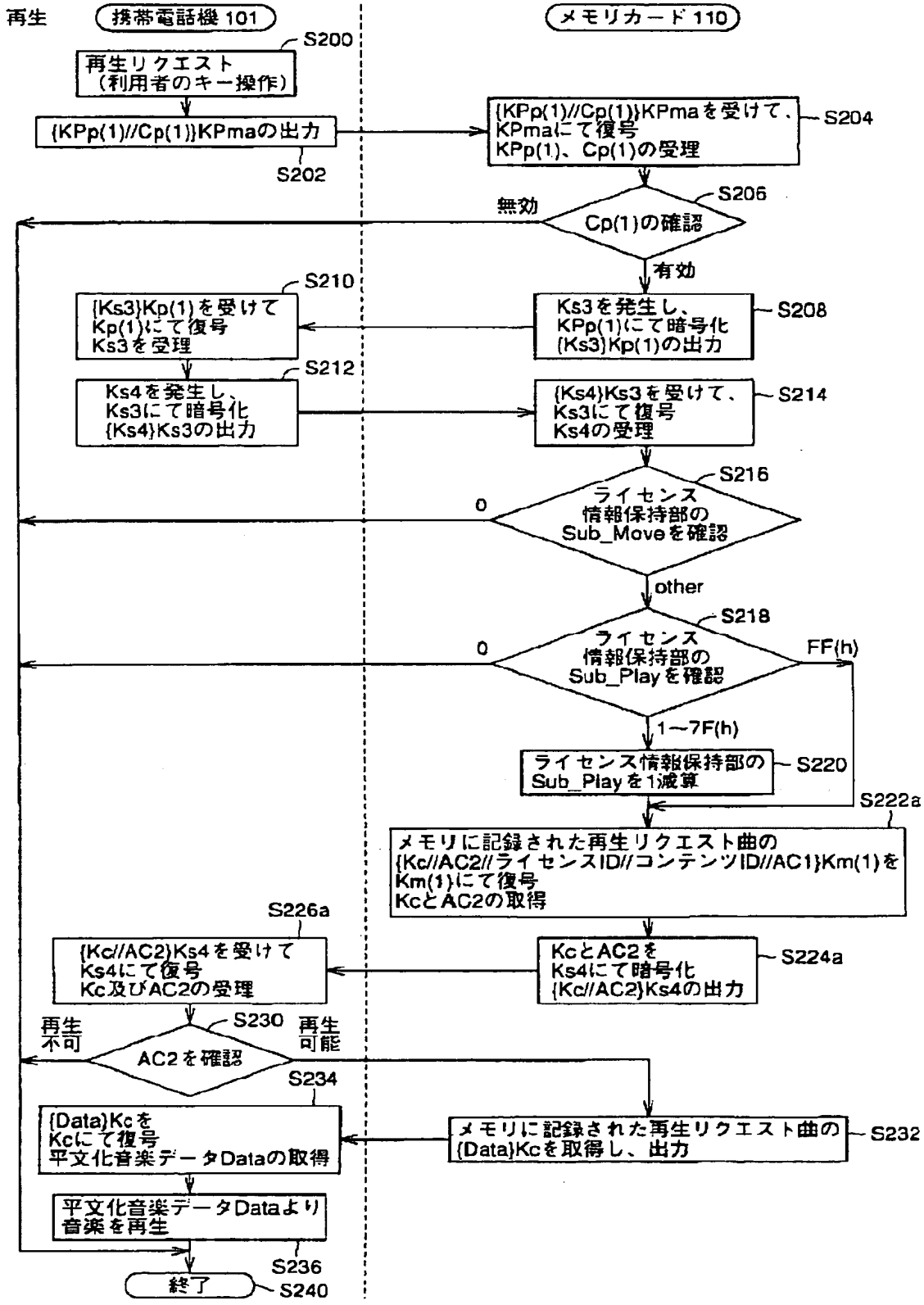
【図１７】

FIG.17


配信
(一部のみ)
S110より
配信サーバ31
携帯電話機101
メモリカード110
S128より
Kc//AC2、ライセンスID、コンテンツIDとAC1を
KPm(1)にて暗号化
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)の生成
S132a
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)を
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)}Ks2の出力
S134a
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)}Ks2の受信
S136a
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)の受理
S138a
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)を
メモリに記録
S140a
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S142a
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S144
コンテンツデータの配信要求
S146
{Data}Kc//Data-infの受信
{Data}Kcと{Data}Kc//Data-infの受理
S150
{Data}Kcと{Data}Kc//Data-infをメモリに記録
S15
{Data}Kcと{Data}Kc//Data-infを
データベースより取得し、
S148
{Data}Kc//Data-infの出力
配信受理を送信
S154
配信受理を受信
S156
配信終了処理
S158
終了
S160

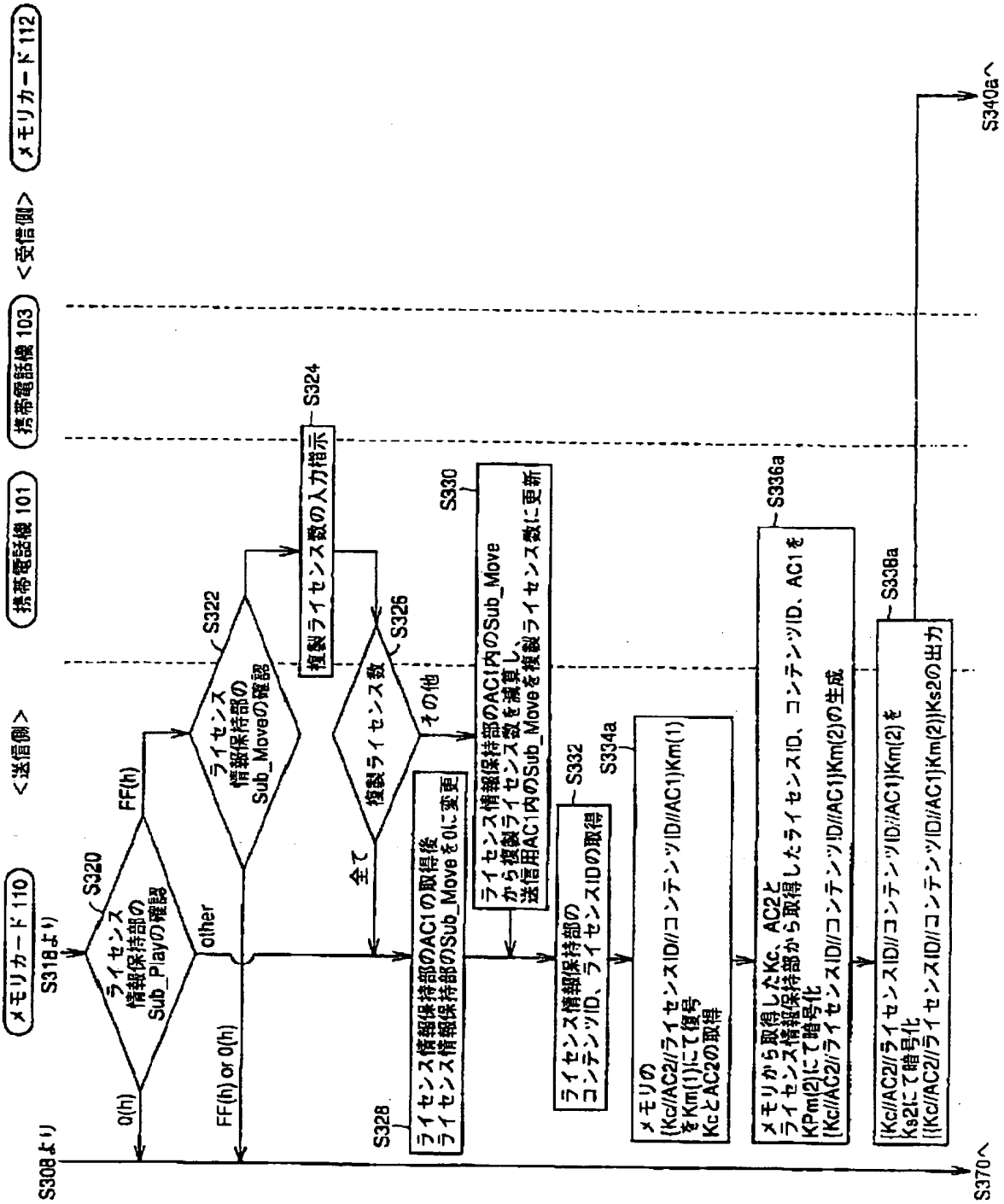
【図１８】

*FIG.18*


再生
携帯電話機 101
メモリカード 110
S200
再生リクエスト
（利用者のキー操作）
{KPp(1)//Cp(1)}KPmaの出力
S202
{KPp(1)//Cp(1)}KPmaを受けて、
KPmaにて復号
KPp(1)、Cp(1)の受理
S204
S206
無効
Cp(1)の確認
有効
S210
{Ks3}Kp(1)を受けて
Kp(1)にて復号
Ks3を受理
S212
Ks4を発生し、
Ks3にて暗号化
{Ks4}Ks3の出力
Ks3を発生し、
KPp(1)にて暗号化
{Ks3}Kp(1)の出力
S208
{Ks4}Ks3を受けて、
Ks3にて復号
Ks4の受理
S214
S216
0
ライセンス
情報保持部の
Sub_Moveを確認
other
S218
0
ライセンス
情報保持部の
Sub_Playを確認
FF(h)
1～7F(h)
ライセンス情報保持部の
Sub_Playを1減算
S220
S222a
メモリに記録された再生リクエスト曲の
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km(1)を
Km(1)にて復号
KcとAC2の取得
S226a
{Kc//AC2}Ks4を受けて
Ks4にて復号
Kc及びAC2の受理
KcとAC2を
Ks4にて暗号化
{Kc//AC2}Ks4の出力
S224a
再生
不可
S230
AC2を確認
再生
可能
S234
{Data}Kcを
Kcにて復号
平文化音楽データDataの取得
メモリに記録された再生リクエスト曲の
{Data}Kcを取得し、出力
S232
平文化音楽データDataより
音楽を再生
S236
終了
S240

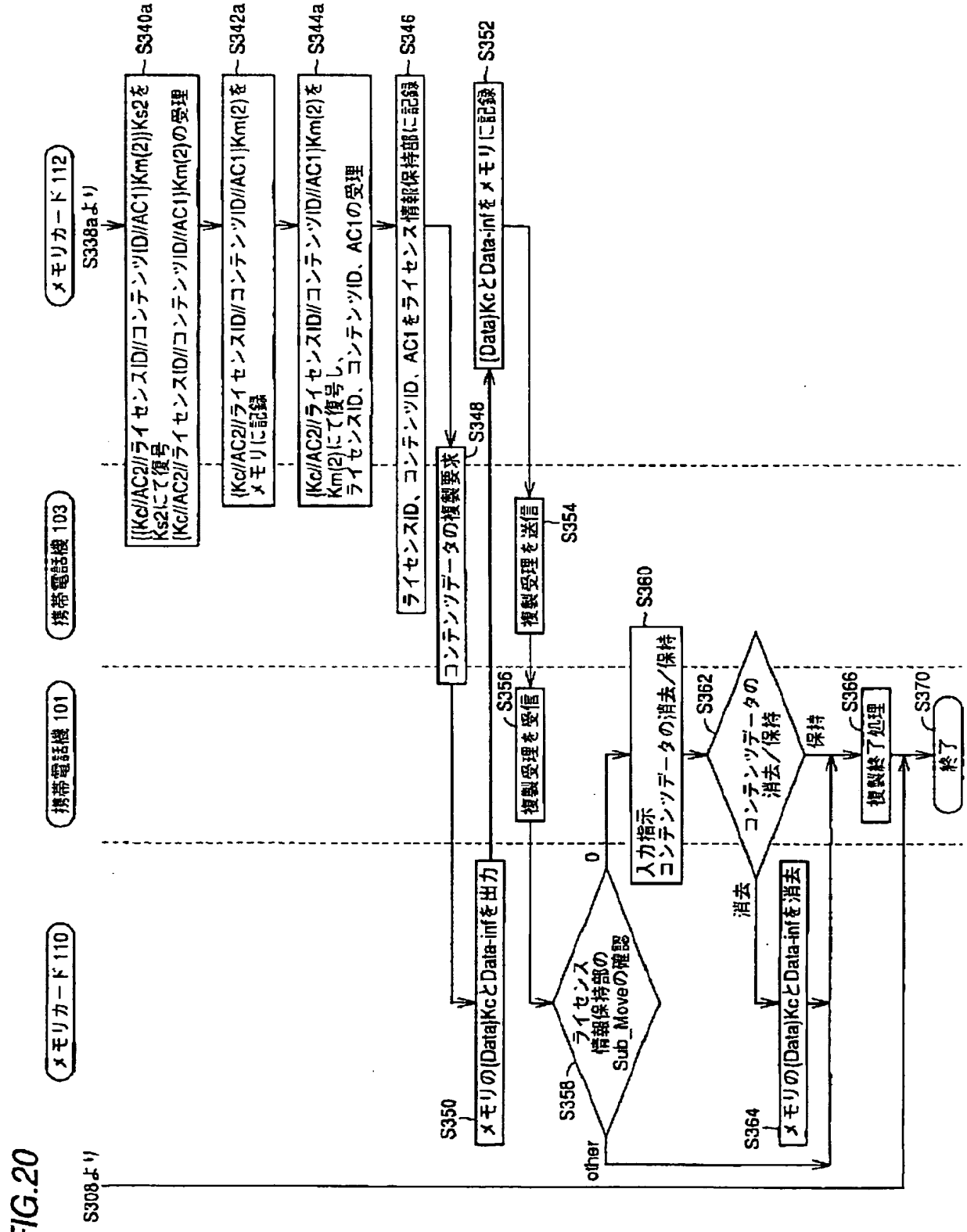
【図１９】

FIG.19


複製
メモリカード 110
<送信側>
携帯電話機 101
携帯電話機 103
<受信側>
メモリカード 112
S308より
S318より
S320
ライセンス情報保持部のSub_Playの確認
0(h)
FF(h)
other
FF(h) or 0(h)
S322
ライセンス情報保持部のSub_Moveの確認
S324
複製ライセンス数の入力指示
全て
複製ライセンス数
S325
その他
S328
ライセンス情報保持部のAC1の取得後ライセンス情報保持部のSub_Moveを0に変更
S330
ライセンス情報保持部のAC1内のSub_Moveから複製ライセンス数を減算し、送信用AC1内のSub_Moveを複製ライセンス数に更新
S332
S334a
ライセンス情報保持部のコンテンツID、ライセンスIDの取得
メモリの{Kc//AC2//ライセンスID//コンテンツID//AC1)Km(1)をKm(1)にて復号KcとAC2の取得
S336a
メモリから取得したKc、AC2とライセンス情報保持部から取得したライセンスID、コンテンツID、AC1をKPm(2)にて暗号化{Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)の生成
S338a
{Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)をKs2にて暗号化{{Kc//AC2//ライセンスID//コンテンツID//AC1)Km(2)}Ks2の出力
S340aへ
S370へ

【図２０】

FIG.20


メモリカード110
携帯電話機101
携帯電話機103
メモリカード112
S308より
S338aより
S340a
{{Kc//AC2}//ライセンスID//コンテンツID//AC1}Km(2)}Ks2を
Ks2にて復号
{Kc//AC2}//ライセンスID//コンテンツID//AC1}Km(2)の受理
S342a
{Kc//AC2}//ライセンスID//コンテンツID//AC1}Km(2)を
メモリに記録
S344a
{Kc//AC2}//ライセンスID//コンテンツID//AC1}Km(2)を
Km(2)にて復号し、
ライセンスID、コンテンツID、AC1の受理
S346
ライセンスID、コンテンツID、AC1をライセンス情報保持部に記録
S348
コンテンツデータの複製要求
S352
{Data}KcとData-infをメモリに記録
S354
複製受理を送信
S356
複製受理を受信
S358
ライセンス
情報保持部の
Sub_Moveの確認
0
other
S360
入力指示
コンテンツデータの消去／保持
S362
コンテンツデータの
消去／保持
消去
保持
S364
メモリの{Data}KcとData-infを消去
S366
複製終了処理
S370
終了
S350
メモリの{Data}KcとData-infを出力

【図２１】

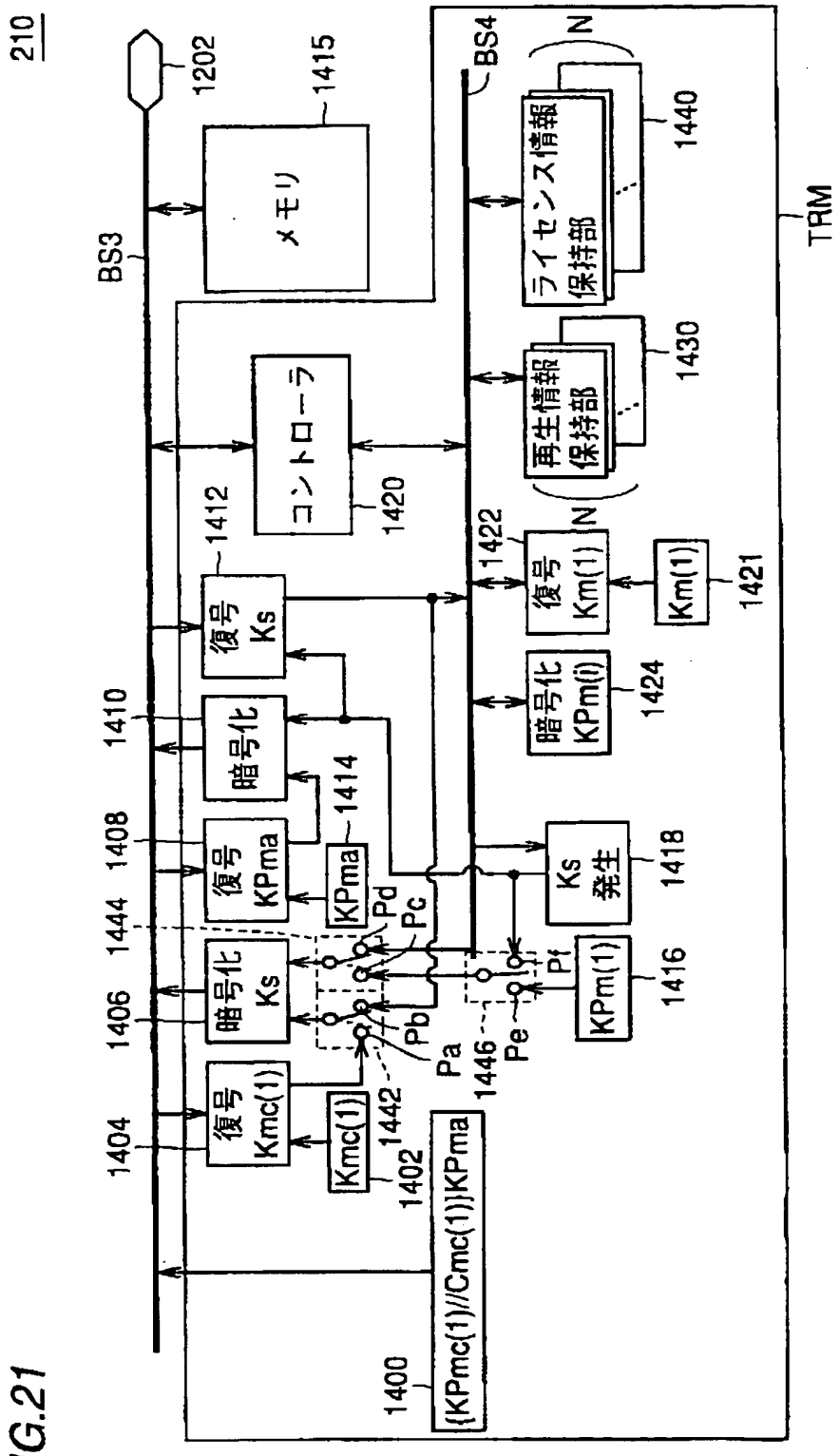
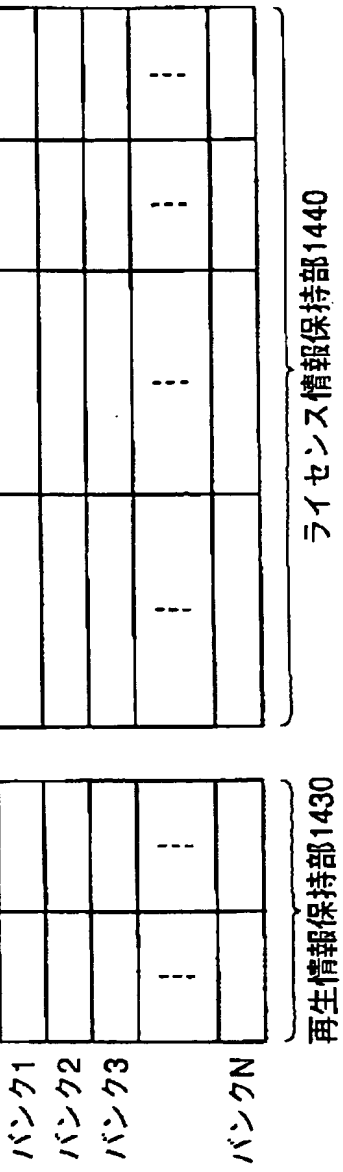

210
1202
1415
メモリ
BS3
BS4
N
ライセンス情報保持部
1440
TRM
1430
再生情報保持部
コントローラ
1420
1412
1422
復号 Ks
復号 Km(1)
Km(1)
1421
1410
暗号化 KPm(i)
1424
暗号化 Ks
1414
1408
復号 KPma
KPma
Pd
Pc
Ks 発生
1418
1444
1406
Pb
Pa
Pf
KPm(1)
1416
1446
Pe
1404
復号 Kmc(1)
Kmc(1)
1442
1402
{KPmc(1)//Cmc(1)}KPma
1400

FIG.21

【図２２】

FIG.22


AC1
Sub_Play Sub_Move
ライセンスID
コンテンツID
ライセンス情報保持部1440
Kc
AC2
再生情報保持部1430
バンク1
バンク2
バンク3
バンクN

【手続補正書】特許協力条約第３４条補正の写し提出書（職権）

【提出日】平成１３年１１月５日（２００１．１１．５）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項１】データ配信システムであって、

暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）を復号して平文のコンテンツデータ（Ｄａｔａ）を得るための復号鍵であるライセンスキー（Ｋｃ）を配信するためのデータ供給装置（１０，１１）と、

前記データ供給装置からの前記配信を受ける複数の端末（１００，１０１）とを備え、

前記データ供給装置は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

前記配信が要求された場合において、アクセス制限情報（ＡＣ１）を生成して、少なくとも前記ライセンスキーを含む再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）と前記アクセス制限情報とを前記第１のインタフェース部を介して配信するための制御を行なう配信制御部（３１５）とを含み、

各前記端末は、

外部との間でデータを授受するための第２のインタフェース部（１１０２）と、

前記第２のインタフェース部を介して、前記データ供給装置から受信した、前記再生情報と前記アクセス制限情報とを記録する配信データ解読装置（１１０，２１０）と、

前記端末の動作を制御するための端末制御部（１１０６）とを含み、

前記配信データ解読装置は、

前記再生情報および前記アクセス制限情報を記録するための記憶部（１４１５

，１４３０，１４４０）と、

前記端末制御部からの前記記憶部に記録された前記再生情報の出力要求がなされた場合、前記記憶部に記録された前記アクセス制限情報に基づいて前記再生情報の出力の可否を判断する制御部（１４２０）とを有し、

前記制御部は、前記再生情報の出力が可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前期アクセス制限情報の変更を行なう、データ配信システム。

【請求項２】各前記端末（１００，１０１）は、

前記端末制御部からコンテンツデータの再生指示がされた場合において、前記配信データ解読装置（１１０，２１０）から前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を受けて、前記ライセンスキー（Ｋｃ）によって前記暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）を復号して再生するためのコンテンツデータ再生部（１５１６，１５１８）をさらに含み、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読装置から前記再生情報を用いて前記暗号化コンテンツデータを復号するために、前記再生情報を出力する出力回数を制限する再生制御情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記端末制御部（１１０６）は、外部からコンテンツデータの再生が指示された場合、前記配信データ解読装置に対して、前記再生情報を用いて前記暗号化コンテンツデータを復号するために前記再生情報の出力を指示する第１の出力要求を行ない、かつ、前記コンテンツ再生部に再生指示を行ない、

前記制御部（１４２０）は、前記端末制御部からの前記第１の出力要求がなされた場合、前記記憶部に記録された前記再生制御情報に基づいて、前記再生情報の出力の可否を判断し、前記再生情報の出力が可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前記再生制御情報の変更を行なう、請求の範囲第１項に記載のデータ配信システム。

【請求項３】前記アクセス制限情報（ＡＣ１）は、前記配信データ解読装置（１１０，２１０）から他の配信データ解読装置（１１２）に対しての、前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力可能回数を規定する複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記端末制御部は、外部から前記再生情報の移動が指示された場合、前記配線データ解読部に対して、他の配信データ解読装置部に対する前記再生情報の出力を指示する第２の出力要求を行ない、

前記制御部（１４２０）は、前記端末制御部からの前記第２の出力要求がなされた場合、他の配信データ解読装置に対して、前記記憶部に記録された前記複製制限情報に基づいて出力の可否を判断し、出力可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前記複製制限情報の変更を行なう、請求の範囲第１項に記載のデータ配信システム。

【請求項４】前記データ供給装置（１０，１１）は、

認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記配信データ解読装置（１１０，２１０）に対応して予め定められる第１の公開暗号鍵（ＫＰｍｃ（ｍ））を、前記第１のインタフェース部（３５０）を介して受けて復号処理するための第１の復号処理部（３１２）と、

前記再生情報の通信ごとに更新される第１の共通鍵（Ｋｓ１）を生成する第１のセッションキー生成部（３１６）と、

前記第１の共通鍵によって暗号化されて、前記第１のインタフェース部を介して返信される第２の公開暗号鍵（ＫＰｍ（ｉ））および第２の共通鍵（Ｋｓ２）を復号抽出するためのセッションキー復号部（３２０）と、

前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記アクセス制限情報（ＡＣ１）を、前記セッションキー復号部により復号された前記第２の公開暗号鍵によって暗号化する第１のライセンスデータ暗号化処理部（３２６）と、

前記第１のライセンスデータ暗号化処理部の出力を、前記セッションキー復号部により復号された前記第２の共通鍵によってさらに暗号化して前記第１のインタフェース部に与え配信するための第２のライセンスデータ暗号化処理部（３２８）とをさらに含み、

前記配信データ解読装置（１１０，２１０）は、

前記認証鍵によって復号可能な状態に暗号化された、前記配信データ解読装置に対応して定められる前記第１の公開暗号鍵を保持し、前記再生情報を新たに記

録する場合に出力する第１の認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号するための第１の秘密復号鍵（Ｋｍｃ（ｍ））を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号鍵によって暗号化された前記第１の共通鍵を受けて、前記第１の秘密復号鍵によって復号処理するための第１の復号処理部（１４０４）と、

前記第２の公開暗号鍵を保持する第２の鍵保持部（１４１６）と、

前記再生情報の通信ごとに更新される前記第２の共通鍵（Ｋｓ２）を生成する第２のセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記第２のインタフェース部（１２０２）に出力するための第１の暗号化処理部（１４０６）と、

前記データ供給装置から配信される、前記第２の共通鍵および前記第２の公開暗号鍵によって暗号化された、前記再生情報および前記アクセス制限情報を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Ｋｍ（ｉ））を保持する第３の鍵保持部（１４２１）と、

暗号化された、前記再生情報および前記アクセス制限情報を、第２の秘密復号鍵によって復号するための第３の復号処理部（１４２２）とをさらに有し、

前記記憶部（１４１５，１４３０，１４４０）は、前記再生情報を、前記第２の公開暗号鍵によって暗号化された状態および前記第３の復号処理部によって復号された状態のいずれか一方の状態で記録するための第１の記憶ブロック（１４１５，１４３０）と、

前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを有する、請求の範囲第１項に記載のデータ配信システム。

【請求項５】前記第２のセッションキー発生部（１４１８）は、前記記憶部に記録された再生情報を用いて前記暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）を復号して再生する再生動作において、第３の共通鍵（Ｋｓ３）を生成し、

前記記憶部（１４１５，１４３０，１４４０）は、前記制御部（１４２０）に制御されて、前記再生動作において、前記再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記再生動作において、前記第１の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を抽出し、

前記第２の復号処理部（１４１２）は、前記再生動作において、前記第３の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記再生情報の通信ごとに更新される第４の共通鍵（Ｋｓ４）を抽出し、

前記第１の暗号化処理部（１４０６）は、前記再生動作において、前記第３の復号処理部および前記第１の記憶ブロックのいずれか一方から前記再生情報を受けて、前記第２の復号処理部（１４１２）で抽出された前記第４の共通鍵によって暗号化し、

各前記端末（１００，１０１）は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

前記認証鍵によって復号可能な状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第３の公開暗号鍵（ＫＰｐ（ｉ））を保持し、前記再生動作に応じて前記配信データ解読装置に対して出力する第２の認証データ保持部（１５００）と、

前記第４の共通鍵を生成する第３のセッションキー発生部（１５０８）と、

前記配信データ解読装置から送信される、前記第４の共通鍵によって暗号化された前記再生情報から前記再生情報を復号抽出するための第４の復号処理部（１５１０）と、

前記再生動作が指示された場合において、前記配信データ解読装置（１１０，２１０）からの前記暗号化コンテンツデータを受けて、前記再生情報に含まれる前記ライセンスキー（Ｋｃ）により前記暗号化コンテンツデータを復号して再生するためのコンテンツデータ再生部（１５１６，１５１８）と、

前記第３の公開暗号鍵によって暗号化されたデータを復号化するための第３の秘密復号鍵（Ｋｐ（ｉ））を保持する第４の鍵保持部（１５０２）と、

前記第３の公開暗号鍵によって暗号化されて前記配信データ解読装置から返信されるデータを復号して前記第３の共通鍵を得るための第５の復号処理部（１５０４）と、

前記第５の復号処理部から受ける前記第３の共通鍵によって、前記第４の共通鍵を暗号化して前記配信データ解読装置に対して出力する第２の暗号化処理部（１５０６）とを有し、

前記配信データ解読装置は、

暗号化された前記第３の公開暗号鍵を前記コンテンツ再生部から受けて、前記認証鍵によって復号処理するための認証処理部（１４０８）と、

前記制御部に制御されて、前記認証処理部から受ける前記第３の公開暗号鍵によって前記第３の共通鍵を暗号化して、対応する前記コンテンツ再生部に対して出力する第３の暗号化処理部（１４１０）とをさらに有し、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読装置から前記再生情報を用いて前記暗号化コンテンツデータを復号して再生するために、前記コンテンツデータ再生部へ前記再生情報を出力する出力回数を制限する再生制御情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記端末制御部（１１０６）は、外部からコンテンツデータの再生が指示された場合、前記配信データ解読装置に対して、前記再生情報を用いて前記暗号化コンテンツデータを復号するために前記再生情報の出力を指示する第１の出力要求を行ない、かつ、前記第１の出力要求に応じて前記配信データ解読装置から出力された前記再生情報および前記暗号化コンテンツデータを前記コンテンツ再生部に与え、　前記制御部（１４２０）は、前記端末制御部からの前記第１の出力要求に応じて、前記再生動作が指示された場合において前記配信データ解読装置の各部の動作を制御し、前記第２の記憶ブロックに記録された前記再生制御情報に基づいて前記再生情報の出力の可否を判断し、前記再生情報の出力が可能と判断した場合、前記再生情報の出力後、必要に応じて前記第２の記憶ブロックに記録された前記再生制御情報の変更を行なう、請求の範囲第４項に記載のデータ配信システム。

【請求項６】前記配信データ解読装置は、

他の配信データ解読装置（１０２）に対して前記再生情報を複製する複製動作において、前記認証鍵によって復号可能な状態に暗号化された前記他の配信データ解読装置に対応する前記第１の公開暗号鍵（ＫＰｍｃ（ｍ））を受けて、前記認証鍵によって復号処理して前記他の配信データ解読装置に対応する前記第１の公開暗号化鍵を抽出する認証処理部（１４０８）と、

前記複製動作において、前記他の配信データ解読装置に対応する前記第１の公開暗号化鍵によって、前記配信データ解読装置の前記第２のセッションキー発生部において発生した前記第３の共通鍵を暗号化して前記他の配信データ解読装置へ出力する第３の暗号化処理部（１４１０）とをさらに有し、

前記配信データ解読装置および前記他の配信データ解読装置にそれぞれ対応する複数の前記第２のセッションキー発生部は、外部から指示される前記複製動作に応じて、前記第３および第２の共通鍵（Ｋｓ３，Ｋｓ２）をそれぞれ生成し、

前記第２の復号処理部（１４１２）は、前記複製動作において、前記配信データ解読装置に対応する前記第３の共通鍵で暗号化されて前記他の配信データ解読装置から返信されるデータを復号して、前記他の配信データ解読装置で生成された前記第２の共通鍵および前記他の配信データ解読装置に対応する前記第２の公開暗号鍵（ＫＰｍ（ｉ））を取得し、

前記第１の記憶ブロック（１４１５，１４３０）は、前記制御部（１４２０）に制御されて、前記複製動作が指示されるのに応じて、前記再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記複製動作において、前記第１の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を抽出し、

前記配信データ解読装置（１１０，２１０）は、

前記複製動作が外部から指示された場合において、前記第３の復号処理部および前記第１の記憶ブロックのいずれか一方から受けた前記再生情報を、前記他の配信データ解読装置に対応する前記第２の公開暗号鍵によって暗号化するための第４の暗号化処理部（１４２４）をさらに有し、

前記第１の暗号化処理部（１４０６）は、前記複製動作において、前記第２の復号処理部（１４１２）によって取得された前記第２の共通鍵と、前記第４の暗

号化処理部の出力とを受けて、前記第４の暗号化処理部の出力を前記第２の共通鍵によってさらに暗号化して前記他の配信データ解読装置に対して出力し、

前記アクセス制限情報（ＡＣ１）は、前記配信データ解読装置（１１０、２１０）から他の配信データ解読装置（１０２，１１２）に対しての、前記再生情報の出力可能回数を規定する複製制限情報（Ｓｕｂ＿ｍｏｖｅ）を含み、

前記端末制御部は、外部から前記再生情報の前記複製動作が指示された場合、前記配信データ解読装置に対して、他の配信データ解読装置に対する前記再生情報の出力を指示する第２の出力要求を行ない、

前記制御部（１４２０）は、前記端末制御部からの前記第２の出力要求がなされた場合、他の配信データ解読装置に対して、前記第２の記憶ブロックに記録された前記複製制限情報に基づいて出力の可否を判断し、出力可能と判断した場合、前記再生情報の出力後、必要に応じて前記第２の記憶ブロックに記録された前記複製制限情報の変更を行なう、請求の範囲第４項に記載のデータ配信システム。

【請求項７】前記データ供給装置（１０）は、

前記コンテンツ再生部にて再生可能な共通秘密鍵（Ｋｃｏｍ）を保持する第５の鍵保持部（３２２）と、

前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を前記共通秘密鍵によって暗号化し、前記第１のライセンスデータ暗号化処理部（３２６）に対して出力する第３のライセンスデータ暗号化部（３２４）とをさらに含み、

前記コンテンツ再生部は、

前記共通秘密鍵を保持する第６の鍵保持部（１５１２）と、

前記第４の復号処理部（１５１０）の出力を受けて、前記第６の鍵保持部に保持された前記共通秘密鍵によって前記再生情報を復号し、前記ライセンスキー（Ｋｃ）を抽出して前記コンテンツデータ再生部（１５１６，１５１８）に対して出力するための第６の復号処理部（１５１４）をさらに有する、請求の範囲第５項に記載のデータ配信システム。

【請求項８】前記データ供給装置（１０）は、

前記コンテンツデータ再生部にて再生可能な第４の公開暗号鍵を保持する第５

の鍵保持部と、

前記再生情報を前記第４の公開暗号鍵にて暗号化し、前記第１のライセンスデータ暗号化処理部に対して出力する第３のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第４の公開暗号鍵によって暗号化された前記再生情報を復号できる第４の秘密復号鍵を保持する第６の鍵保持部と、

前記第４の復号処理部の出力を受けて、前記第６の鍵保持部に保持された前記第４の秘密復号鍵によって前記再生情報（ＡＣ／／Ｋｃ２）を復号し、前記ライセンスキー（Ｋｃ）を抽出して前記コンテンツデータ再生部（１５１６，１５１８）に対して出力するための第６の復号処理部をさらに含む、請求の範囲第５項に記載のデータ配信システム。

【請求項９】前記配信データ解読装置（１１０，２１０）は、前記端末（１００，１０１）に着脱可能な記録装置である、請求の範囲第１項に記載のデータ配信システム。

【請求項１０】前記記録装置は、メモリカードである、請求の範囲第９項に記載のデータ配信システム。

【請求項１１】前記第１のインタフェース部（３５０）と前記第２のインタフェース部（１２０２）とは、携帯電話網によって接続される、請求の範囲第１項に記載のデータ配信システム。

【請求項１２】前記記憶部（１４１５，１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１３】前記配信データ解読装置（１１０）は、暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）をさらに記録し、

前記記憶部（１４１５，１４４０）は、

前記暗号化コンテンツデータおよび暗号化された状態の前記再生情報を記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを

含み、

前記第２の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１４】前記配信データ解読装置（１１０）は、暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）をさらに記録し、

前記記憶部（１４１５，１４３０，１４４０）は、

前記暗号化コンテンツデータを記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報および前記再生情報を記録するための第２の記憶ブロック（１４３０，１４４０）とを含み、

前記第２の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１項に記載のデータ配信システム。

【請求項１５】前記配信データ解読装置（１１０，１２０）は、

前記配信データ解読装置に対して予め付与された認証データを保持する認証データ保持部（１４００）をさらに有し、

前記端末制御部は、前記認証データを前記第２のインタフェースを介して、前記データ供給装置に対して送信するように指示し、

前記配信制御部（３１５）は、送信されてきた配信先の前記端末の前記認証データを前記第１のインタフェースを介して受信し、受信した前記認証データに基づいて配信先の前記配信データ解読装置（１１０，１２０）の認証処理を行ない、認証した場合、前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）と前記アクセス制限情報（ＡＣ１）とを前記第１のインタフェース部（３５０）を介して出力する、請求の範囲第１項に記載のデータ配信システム。

【請求項１６】前記配信データ解読装置（１１０，１２０）は、前記再生情報の出力要求がなされた場合、前記再生情報の出力先から認証データを受け取り、受け取った前記認証データに基づいて出力先の認証処理を行ない、認証した場合、前記再生情報を出力し、

前記端末制御部は、前記配信データ解読装置から出力された前記再生情報を前記第２のインタフェース部（１１０２）を介して出力する、請求の範囲第１項に

記載のデータ配信システム。

【請求項１７】前記制御部（１４２０）は、前記第２の出力要求に対して、他の配信データ解読装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の配信データ解読装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の配信データ解読装置に対して出力する、請求の範囲第３項に記載のデータ配信システム。

【請求項１８】前記制御部（１４２０）は、前記第２の出力要求に対して、他の配信データ解読装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の配信データ解読装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第４の暗号化処理部は、変更した前記アクセス制限情報を暗号化して、前記再生情報とともに前記第１の暗号化処理部へ与える、請求の範囲第６項に記載のデータ配信システム。

【請求項１９】暗号化データ（｛Ｄａｔａ｝Ｋｃ）を復号して平文のデータ（Ｄａｔａ）を得るための復号鍵であるライセンスキー（Ｋｃ）を含む前記暗号化データの再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）を格納する記録装置であって、

外部との間でデータを授受するためのインタフェース部（１２０２）と、

前記再生情報および前記再生情報の前記記録装置からの出力を制御するためのアクセス制限情報（ＡＣ１）を記録するための記憶部（１４１５，１４３０，１４４０）と、

外部から前記記憶部に記録された前記再生情報の出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記再生情報の出力の可

否を判断する制御部（１４２０）とを備え、

前記制御部は、前記再生情報の出力が可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前記アクセス制限情報の変更を行なう、記録装置。

【請求項２０】前記アクセス制限情報（ＡＣ１）は、前記記録装置から前記再生情報を用いて前記暗号化データを再生するために、前記再生情報を出力する出力回数を制限する再生制御情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記制御部（１４２０）は、前記再生情報を用いて前記暗号化データを再生するための前記再生情報の出力が外部から指示された場合において、前記記憶部に記録された前記再生制御情報に基づいて、前記再生情報の出力の可否を判断し、前記再生情報の出力が可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前記再生制御情報の変更を行なう、請求の範囲第１９項に記載の記録装置。

【請求項２１】前記アクセス制限情報（ＡＣ１）は、他の前記記録装置（１１２）に対する前記再生情報（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力回数を規定する複製可能回数を制限する複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記制御部（１４２０）は、前記他の記録装置に対する前記再生情報の出力指示が外部から指示された場合において、前記記憶部に記録された前記複製制限情報に基づいて出力の可否を判断し、出力可能と判断した場合、前記再生情報の出力後、必要に応じて前記記憶部に記録された前記複製制限情報の変更を行なう、請求の範囲第１９項に記載の記録装置。

【請求項２２】前記記録装置は、

前記記録装置に対応して予め定められる公開暗号鍵（ＫＰｍ（ｉ））によって暗号化されたデータを復号するための秘密復号鍵（Ｋｍ（ｉ））を保持する秘密鍵保持部（１４２１）と、

前記インタフェース部（１２０２）を介して入力される、前記公開暗号鍵によって暗号化された前記アクセス制限情報（ＡＣ１）を復号して、前記記憶ブロックに与えるアクセス制限情報復号部（１４２２）とをさらに備え、

前記記憶部は、

前記アクセス制限情報（ＡＣ１）を記録するための第１の記憶ブロック（１４４０）と、

前記公開暗号鍵によって暗号化された前記再生情報を記録する第２の記憶ブロック（１４１５）とを有し、

前記第１の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１９項に記載の記録装置。

【請求項２３】前記記憶部は、

前記アクセス制限情報（ＡＣ１）を記録するための第１の記憶ブロック（１４４０）と、

前記再生情報を記録する第２の記憶ブロック（１４１５）とを有し、

前記第１および第２の記憶ブロック（１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第１９項に記載の記録装置。

【請求項２４】記録装置であって、

外部との間でデータを授受するためのインタフェース部（１２０２）と、

前記インタフェース部を介して入力される、格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記格納データの前記記録装置からの出力を制御するためのアクセス制限情報（ＡＣ１）を記録するための記憶部（１４１５，１４３０，１４４０）と、

認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記記録装置に対応して定められる第１の公開暗号鍵（ＫＰｍｃ（ｍ））を保持し、前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）および前記アクセス制限情報（ＡＣ１）を受信する場合において前記インタフェース部（１２０２）を介して外部に出力する認証データ保持部（１４００）と、

前記第１の公開暗号鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵（Ｋｍｃ（ｍ））を保持する第１の鍵保持部（１４４２）と、

前記第１の公開暗号鍵によって暗号化された第１の共通鍵（Ｋｓ１）を前記インタフェース部を介して外部から受けて、復号処理するための第１の復号処理（

１４０４）と、

前記記録装置ごとに異なる第２の公開暗号鍵（ＫＰｍ（ｉ））を保持する第２の鍵保持部（１４１６）と、

前記格納データの通信ごとに更新される第２の共通鍵（Ｋｓ２）を生成するセッションキー発生部（１４１８）と、

前記第２の共通鍵および前記第２の公開暗号鍵を前記第１の共通鍵によって暗号化し、前記インタフェース部を介して外部に出力するための第１の暗号化処理部（１４０６）と、

前記インタフェース部を介して、前記第２の共通鍵および前記第２の公開暗号鍵によって暗号化されて入力される前記格納データおよび前記アクセス制限情報を受けて、前記第２の共通鍵によって復号するための第２の復号処理部（１４１２）と、

前記第２の公開暗号鍵によって暗号化されたデータを復号するための第２の秘密復号鍵（Ｋｍ（ｉ））を保持する第３の鍵保持部（１４２１）と、

暗合化された、前記格納データおよび前記アクセス制限情報を、前記第２の秘密復号鍵によって復号するための第３の復号処理部（１４２２）と、

外部から前記記憶部に記録された前記格納データの出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記格納データの再生情報の出力の可否を判断する制御部（１４２０）とを備え、

前記記憶部（１４１５，１４３０，１４４０）は、前記格納データを、前記第２の公開暗号鍵によって暗号化された状態および、前記第３の復号処理部によって復号された状態のいずれか一方の状態で記録し、

前記制御部は、前記格納データの出力が可能と判断した場合、前記格納データの出力後、必要に応じて前記部に記録された前記アクセス制限情報の変更を行なう、記録装置。

【請求項２５】前記アクセス制限情報は、前記記録装置から他の機器への前記格納データの出力回数を制限する出力回数制限情報（Ｓｕｂ＿Ｐｌａｙ）を含み、

前記セッションキー発生部（１４１８）は、外部から指示される、他の機器（１００，１０１）への前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋ

ｃｏｍ）の出力指示である第１の出力指示に応じて、第３の共通鍵（Ｋｓ３）を生成し、

前記記録装置は、

前記認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記他の機器に対応して予め定められる第３の公開暗号鍵（ＫＰｐ（ｎ））を前記インタフェース部（１２０２）を介して受けて、前記認証鍵によって復号処理するための認証処理部（１４０８）と、

前記第１の出力指示に応じて、前記認証処理部から受ける前記第３の公開暗号鍵によって前記第３の共通鍵を暗号化して、前記他の機器に対して出力する第２の暗号化処理部（１４１０）とをさらに備え、

前記インタフェース部は、前記第１の出力指示に応じて、前記第３の共通鍵によって暗号化されて返信される、前記他の機器において生成された第４の共通鍵（Ｋｓ４）を受けて前記第２の復号処理部（１４１２）に伝達し、

前記第２の復号処理部は、前記第１の出力指示に応じて、前記セッションキー発生部から受けた前記第３の共通鍵によって、前記第３の共通鍵によって暗号化された前記第４の共通鍵（Ｋｓ４）を抽出し、

前記記憶部は、前記制御部（１４２０）に制御されて、前記第１の出力指示に応じて、前記格納データを出力し、

前記第３の復号処理部（１４２２）は、前記第１の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって前記格納データを抽出し、

前記第１の暗号化処理部（１４０６）は、前記第１の出力指示に応じて、前記第３の復号処理部および前記記憶部のいずれか一方から前記格納データを受けて、前記第２の復号処理部（１４１２）で抽出された前記第４の共通鍵によって暗号化して、前記インタフェース部を介して前記他の機器に出力し、

前記制御部（１４２０）は、前記第１の出力指示に応じて前記記録装置内の各部の動作を制御し、前記アクセス制限情報に基づいて前記格納データの出力の可否を判断し、前記記憶部に記録された前記出力回数制限情報に基づいて前記格納データの出力の可否を判断し、出力可能と判断した場合、前記格納データの出力

後、必要に応じて前記記憶部に記録された前記出力回数制限情報の変更を行なう、請求の範囲第２４項に記載の記録装置。

【請求項２６】前記アクセス制限情報は、前記記録装置から他の記録装置への前記格納データの出力回数を制限する複製回数制限情報（Ｓｕｂ＿Ｍｏｖｅ）を含み、

前記セッションキー発生部（１４１８）は、外部から指示される、前記記録装置から他の記録装置（１１２）への前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）の出力指示である第２の出力指示に応じて、前記第３の共通鍵（Ｋｓ３）を生成し、

前記記録装置は、

前記認証鍵（ＫＰｍａ）によって復号可能な状態に暗号化された、前記他の記録装置に対応する前記第１の公開暗号鍵（ＫＰｍｃ（ｍ））を前記インタフェース部（１２０２）を介して受けて、復号処理によって取得する認証処理部（１４０８）と、

前記第２の出力指示に応じて、他の記録装置に対応する前記第１の公開暗号鍵によって、前記セッションキー発生部で生成された前記第３の共通鍵を暗号化して、前記他の記録装置に対して出力する第２の暗号化処理部（１４１０）とをさらに備え、

前記インタフェース部は、前記第２の出力指示に応じて、前記第３の共通鍵によって暗号化されて返信される、前記他の記録装置において生成された第４の共通鍵（Ｋｓ４）を受けて前記第２の復号処理部（１４１２）に伝達し、

前記第２の復号処理部（１４１２）は、前記第２の出力指示に応じて、前記記録装置に対応する前記第３の共通鍵で暗号化されて前記他の記録装置から返信されるデータを復号して、前記他の記録装置で生成された前記第２の共通鍵（Ｋｓ２）および前記他の記録装置に対応する前記第２の公開暗号鍵（ＫＰｍ（ｉ））を取得し、

前記記憶部は、前記制御部（１４２０）に制御されて、前記第２の出力指示に応じて、前記格納データを出力し、

前記第３の復号処理部（１４２２）は、前記第２の出力指示に応じて、前記記

憶部から出力された前記格納データが暗号化されている場合に、復号を行なって前記格納データを抽出し、

前記記録装置は、

前記第２の出力指示がなされた場合において、前記第３の復号処理部および前記記憶部のいずれか一方から受けた前記格納データを、前記他の記録装置に対応する前記第２の公開暗号鍵によって暗号化するための第３の暗号化処理部（１４２４）をさらに有し、

前記第１の暗号化処理部（１４０６）は、前記第２の出力指示に応じて、前記第３の暗号化処理部の出力を、前記他の記録装置で生成された前記第２の共通鍵によってさらに暗号化して、前記インタフェース部を介して前記他の記録装置に出力し、

前記制御部（１４２０）は、外部からの前記第２の出力指示に応じて前記記録装置内の各部の動作を制御し、前記記憶部に格納された前記複製回数制限情報に基づいて前記格納データの出力を判断し、出力可能と判断した場合、前記格納データの出力後、必要に応じて前記記憶部に格納された前記複製回数制限情報の変更を行なう、請求の範囲第２４項に記載の記録装置。

【請求項２７】前記記憶部（１４１５，１４３０，１４４０）は、前記インタフェース部（１２０２）を介して外部から入力される暗号化コンテンツデータ（｛Ｄａｔａ｝Ｋｃ）をさらに記録し、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）は、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Ｄａｔａ）を得るための復号鍵であるライセンスキー（Ｋｃ）を含む、請求の範囲第２４項に記載の記録装置。

【請求項２８】前記記録装置は、メモリカードである、請求の範囲第２４項に記載の記録装置。

【請求項２９】前記記憶部（１４１５，１４３０，１４４０）は、外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される、請求の範囲第２４項に記載の記録装置。

【請求項３０】記憶部（１４１５，１４３０，１４４０）は、

外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される第１の記憶ブロック（１４３０，１４４０）と、

外部から直接アクセス可能な第２の記憶ブロック（１４１５）とを含み、

前記アクセス制限情報（ＡＣ１）は、前記第１の記憶ブロックに記録され、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）は、暗号化されて前記第２の記憶ブロックに記録される、請求の範囲第２４項に記載の記録装置。

【請求項３１】記憶部（１４１５，１４３０，１４４０）は、

外部から直接アクセス不可能なセキュリティー領域（ＴＲＭ）内に配置される第１の記憶ブロック（１４３０，１４４０）と、

外部から直接アクセス可能な第２の記憶ブロック（１４１５）とを含み、

前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）およびアクセス制限情報（ＡＣ１）は、前記第１の記憶ブロックに記録される、請求の範囲第２４項に記載の記録装置。

【請求項３２】前記記録装置（１１０，１２０）は、前記再生情報の出力が指示された場合、前記再生情報の出力先から認証データを受け取り、受け取った前記データに基づいて、出力先の認証処理を行ない認証した場合に前記再生情報を出力する、請求の範囲第１９項に記載の記録装置。

【請求項３３】前記制御部（１４２０）は、他の記録装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の記録装置に対して出力する、請求の範囲第２１項に記載の記録装置。

【請求項３４】前記制御部（１４２０）は、前記第２の出力指示において、他の記録装置（１１２）に対しての前記アクセス制限情報（ＡＣ１）を前記格納データ（Ｋｃ／／ＡＣ２，｛Ｋｃ／／ＡＣ２｝Ｋｃｏｍ）とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報（Ｓｕｂ＿Ｍｏｖｅ）を生成するとともに、前記記憶部（１４１５，１４３０，１４３０）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第３の暗号化処理部は、前記格納データとともに、変更した前記アクセス制限情報を暗号化し、前記第１の暗号化処理部へ与える、請求の範囲第２６項に記載の記録装置。

【請求項３５】前記記憶部（１４１５，１４３０，１４４０）は、前記インタフェース部（１２０２）を介して暗号化データ（｛Ｄａｔａ｝Ｋｃ）を記録する第３の記憶ブロックをさらに有し、

前記第３の記憶ブロックは、前記インタフェースを介して外部からアクセス可能である、請求の範囲第２３項に記載の記録装置。

【請求項３６】前記記憶部（１４１５，１４３０，１４４０）は、前記インタフェース部（１２０２）を介して暗号化データ（｛Ｄａｔａ｝Ｋｃ）を記録する第３の記憶ブロックをさらに有し、

前記第３の記憶ブロックは、前記インタフェースを介して外部からアクセス可能である、請求の範囲第２４項に記載の記録装置。

【国際調査報告】

| 国際調査報告 | 国際出願番号 PCT/JP00/08593 |
|---|---|

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl'
H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

B. 調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl'
H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2001年
日本国登録実用新案公報 1994-2001年
日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）
WPI（DIALOG）
INSPEC（DIALOG）

C. 関連すると認められる文献

| 引用文献のカテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | JP, 10-3745, A（ソニー株式会社）<br>6. 1月. 1998（06. 01. 98）<br>& EP, 813194, A & CN, 1182268, A | 1-3, 9-17, 19-23, 27-33 |
| Y | 芳尾太郎“小型メモリ・カードで音楽著作権を守る”<br>日経エレクトロニクス, No. 739, (1999年3月), pp. 49-53 | 1-3, 9-17, 19-23, 27-33 |
| Y | 芳尾太郎“実用期の配信システム、著作権管理がカギ握る”<br>日経エレクトロニクス, No. 738, (1999年3月), pp. 94-98 | 1-3, 9-17, 19-23, 27-33 |

☑ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

| 国際調査を完了した日 | 国際調査報告の発送日 |
|---|---|
| 08. 03. 01 | 21.03.01 |

| 国際調査機関の名称及びあて先 | 特許庁審査官（権限のある職員） | 5W | 9570 |
|---|---|---|---|
| 日本国特許庁（ISA/JP）<br>郵便番号100-8915<br>東京都千代田区霞が関三丁目4番3号 | 丸山 高政<br>電話番号 03-3581-1101 内線 3574 | | |

様式PCT/ISA/210（第2ページ）（1998年7月）

| 国際調査報告 | 国際出願番号 PCT/JP00/08593 |
|---|---|

C（続き）. 関連すると認められる文献

| 引用文献のカテゴリー* | 引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | JP, 11-164058, A (日立電子サービス株式会社) 18. 6月. 1999 (18. 06. 99), (ファミリーなし) | 11 |
| A | JP, 11-328850, A (ソニー株式会社) 30. 11月. 1999 (30. 11. 99) & WO, 99/59092, A1 & EP, 996074, A | 1-34 |

フロントページの続き

| (51)Int.Cl.[7] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| G06K | 17/00 | | G06K | 17/00 | L |
| | 19/00 | | G09C | 1/00 | 660A |
| | 19/07 | | G10K | 15/02 | |
| G09C | 1/00 | 660 | H04L | 9/00 | 601B |
| G10K | 15/02 | | | | 601E |
| H04L | 9/08 | | G06K | 19/00 | Q |
| | | | | | N |

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(71)出願人 コロムビアミュージックエンタテインメント株式会社
東京都港区赤坂４丁目14番14号
(72)発明者 堀 吉宏
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 日置 敏昭
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 金森 美和
大阪府守口市京阪本通２丁目５番５号 三洋電機株式会社内
(72)発明者 高橋 政孝
石川県河北郡宇ノ気町字宇野気ヌ98番地の２ 株式会社ピーエフユー内
(72)発明者 長谷部 高行
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内
(72)発明者 吉岡 誠
神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内

(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　利根川　忠明
東京都小平市上水本町五丁目20番１号　株式会社日立製作所　半導体グループ内
(72)発明者　穴澤　健明
東京都港区赤坂四丁目14番14号　日本コロムビア株式会社内

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。

なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項（実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。